Collaborative Informatics Security in Distributed Systems

ION IVAN, MIHAI DOINEA, CRISTIAN CIUREA, CATALIN SBORA
Department of Economic Informatics and Cybernetics
University of Economic Studies
Piata Romana 6, Bucharest, ROMANIA
ionivan@ase.ro, mihai.doinea@ie.ase.ro, cristian.ciurea@ie.ase.ro, catalin.sbora@gmail.com

Abstract: - This paper presents the features of distributed systems in the knowledge-based society. There are identified security special requirements for distributed informatics applications oriented on integration processes. There are established criteria for measuring the performance level for distributed collaborative systems, given that informatics security has also collaborative character. For the banking systems, a collaborative informatics security solution is proposed.

Key-Words: -security, collaborative, distributed system, informatics, banking.

1 Distributed informatics systems in the knowledge-based society

The outcome of knowledge based society is nonetheless a mixture of multidisciplinary sciences that contribute with their instruments in achieving a collaborative objective. E-science, as presented in [1], is driven by three main forces: computing power, network bandwidth and data storage capacity. The technological perspectives of this approach are:

- computing power is doubling every two years in terms of number of transistors, respecting every word of Moore's law [2] which says that the number of transistors per integrated circuits will double almost every two years;
- network bandwidth doubles every year and the storage capacity is almost unlimited in terms of being able to write and transport digital material without any problems, as a direct consequence of Moore's law;
- security threats are a growing concern since the complexity of the collaborative processes increases almost exponentially.

Given these directions all human activities have embraced the computing power, and sciences had turned into a big and powerful bubble, capable to unite all things under a common and interdisciplinary name, called E-science.

In [3] is considered that the world is already living in a knowledge-based society and do not have a theory of the knowledge-based society. Also there still exists a methodological gap about the empirical indicators.

Basically in modern societies almost all the activities are based on different forms of knowledge either if we are talking about theoretical or practical knowledge. The development of such society is sustained by the progress that information technology has made in the last 25 years, the development of the Internet as a global network and the expansion of wired and wireless communication has managed to break cultural, social and geographical barriers placing western societies, that have managed to reach a higher degree of evolution over the years, in the same global context as the underdeveloped or in course of development societies. The low cost of the working force in the emergent countries makes the entrepreneurs in the advanced countries to externalize some of their work to emergent countries, but with the work they are also exporting the knowledge needed to complete the tasks involved by the requirements, balancing the knowledge on a global scale, and this is a great contribution on the evolution of the human society overall. Considering the above statements we have the following characteristics of the knowledge based society:

- globalization, meaning the unification of cultures, ideas and economic activities;
- collaboration, meaning the communication, coordination and cooperation between different entities;
- self-organization, meaning the auto-management of own activities and resources.

Although the things don't seem to be complicated, at some point the amount of knowledge that must be handled is overwhelming and systems for knowledge management must be used for an efficient use of the information.

In [4] is considered that the knowledge management aims to solve the generation,

representation, storage, distribution and application of knowledge. These are very important in network organizations and in the distributed work. In order to support cooperation over distance, advanced databases are used, but the use of technology cannot replace tacit forms of knowledge in the case of critical work situations.

In this global approach of knowledge the most appropriate technology for managing the information is related to distributed systems. Christos Kloukinas, in the course that he holds at City University London, presents the distributed systems as having the following characteristics:

- a distributed system has multiple autonomous components;
- a distributed system has heterogeneous components;
- not all components are shared by all users;
- there is the possibility that resources may not be accessible;
- software runs in concurrent processes on different processors;
- multiple points of control;
- multiple points of failure (but more fault tolerant).

In the context of knowledge based society, distributed systems are widely used for sharing information. The most common used distributed system in today's society is the Internet, seen as a huge network with the information, applications and the hardware distributed geographically around the globe. With these characteristics, the Internet complies with Enslow's definition for distributed systems, as it can be seen in Figure 1.

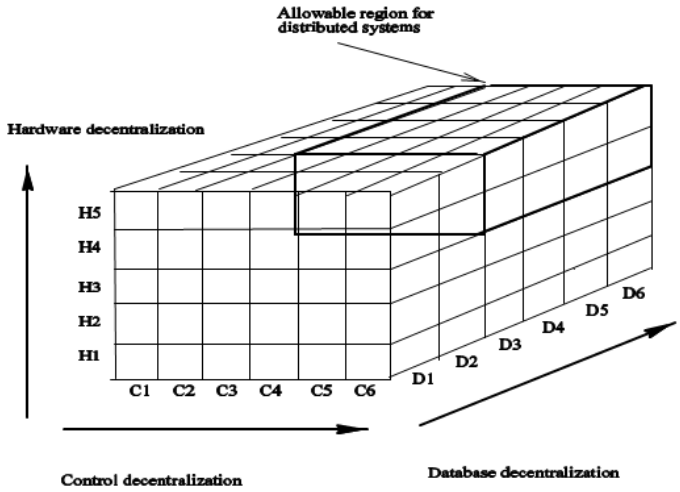

Fig. 1. Enslow's representation of distributed systems [7]

According to Enslow's definition, a system can be classified as a distributed system if the hardware, control and data components have a certain degree of decentralization [7].

The evolution of mobile devices and mobile Internet has become the new factor that contribute to the development of a knowledge oriented society. Mobile devices are offering the possibility of being in a permanent contact with sources of information and also, almost a permanent communication is possible in the cases were needed, improving collaboration experience. As a consequence collaboration through mobile devices has become an important factor for increasing the speed of developing new products and technologies. Having many common services available (like billing systems, tax collecting systems) for a large scale use it will reduce the time spent by one person, doing something else than focusing on problems that are really important.

The new systems of sharing information are offering the necessary conditions for a continuous and innovative development, allowing distributing general interest information on a large scale. The information is the most important factor in the evolution of a group, in the sense of creating and developing new products that will help in a day by day activity. In a knowledge based society it is important that before the process of sharing information, a process of creating and generating new information to take place, in other words it is important that the new information being shared to have an innovative character.

The evolution in a society based on knowledge is rather fast and sometimes it requires some additional effort to keep the pace with the newest information and adapt to the new reality.

Distributed informatics systems, from the knowledge-based society, are knowledge management systems that follow the systems from information society. They are ordered systems, which include procedures that uniform governs the relationships between components. In the knowledge society, the human component plays a particularly high role on the behavior of each element of the distributed informatics system. In this context, to the classical distributed systems, characterized by the possibility of executing common activities from separate locations, new features are added, such as communication, coordination and cooperation, in order to integrate them in the requirements of the knowledge-based society.

2 Collaborative informatics security

The informatics security is an important issue that must be analyzed in order to identify security requests, to discover possible vulnerabilities or threats and to avoid loss of information [5].

The informatics security requires the existence of the followings [6]:

- *confidentiality*, which means protecting data leaking to unauthorized parties, such as personal identification data or credit card information;
- *integrity*, that suppose avoiding data corruption and keeping data integrity;
- *availability*, which means ensuring that data and applications can always be accessed, regardless of any interferences, to authorized entities.

In the context of complex distributed informatics systems for the knowledge-based society, the informatics security is oriented on collaborative side, which means that security components cooperate to achieve a common goal, represented by vulnerabilities elimination.

The need of collaboration for ensuring the security process comes from the multiple sources of threats. Since most of the times it is impossible for one security technology to cover all of those sources, it is important to create components that address different security aspects. Usually the collaborative components are united by a well-defined security management process.

Fig. 2. Security Management cycle [8]

A security management process must have at least 4 phases:

- *Prevent* – use of active security solutions that will identify security threats and it will block them;
- *Detect* – use of active solutions capable of detecting security risks that the systems are being exposed to, due to missing / insecure components;
- *Report*–use of software components in order to create human readable statistics and documents that will help in finding vulnerable points of failure; the information generated at this step is strongly dependent by the prevent and detect components, as the output resulted from this phase is based on the input that is coming from the previously mentioned components;
- *Remediate* – use of software resources for undoing damages and for covering security flaws; usually for undoing the damages, back-up copies for the components are needed, while for covering security flaws, most of the times, software patches will be applied.

Informatics security is an area that deals with controls, procedure and standards applied in informational society for increasing the relevancy degree of data, information and knowledge. Informatics security is an approach to which most of the organizations are repellent, having no concerns about their information system's protection. For this reason many organizations suffer losses, greater than the actual costs of the security implementation process, which represents a main criterion for security optimization, as depicted in Figure 3.

Fig. 3. The balance between security and non-security costs

Collaborative informatics security comes to enforce the knowledge based society oriented information systems, that are continuously threaten by the outside and inside existing threats. Collaborative informatics security is defined as a mixture of security equipment working together for achieving the same objective, meaning a balance between the security costs for risk avoidance procedures and the costs generated by a non-security policy scenario. Due to its major advantages given by its ease of communication between the components of a collaborative system, collaborative informatics security achieves scalability by integrating into the system a new artifact that can centralize all messages received from individual components and run a security diagnostic, balancing in this way the security resources.

Let $R_1, R_2, \ldots, R_n$ be the security resources for a collaborative system. Let $SR_1, SR_2, \ldots, SR_m$ be the risks associated with the collaborative system. Let SCM be the security correlation matrix between the defined security resources, $R_i, i = \overline{1,n}$ and the collaborative system associated risks, $SR_j, j = \overline{1,m}$ as depicted in Table 1.

Table 1. Correlation matrix between security resources and associated risks

	SR_1	...	SR_j	...	SR_m
R_1	scm_{11}	...	scm_{1j}	...	scm_{1m}
...	...	...	...	...	...
R_i	scm_{i1}	...	scm_{ij}	...	scm_{im}
...	...	...	...	...	...
R_n	scm_{n1}	...	scm_{nj}	...	scm_{nm}
	$\sum_{i=1}^{n} scm_{i1} \le NSR_1$	...	$\sum_{i=1}^{n} scm_{ij} \le NSR_j$	...	$\sum_{i=1}^{n} scm_{im} \le NSR_m$

Each security risk $SR_j, j = \overline{1,m}$, has a necessary of resources associated, NSR_j, $j = \overline{1,m}$, that must be covered in order to have a safe working environment in the collaborative system.

Each scm_{ij} element of the matrix represents the quantity of resources of *i* category used in combating the security risks of *j* category, meaning that the $\sum_{i=1}^{n} scm_{ij}$ formula gives how many resources from different types are used in neutralizing an entire security risk category.

In a security process is important to be aware of the needs and resources that the protected infrastructure has, in order to adapt security policies in such way that this process will have the lowest possible interference with the normal business flow.

3 Collaborative security metrics

Collaborative security requires the construction of a set of indicators based on which, relevant information can be extracted from the system, regarding:

- measurements upon the behavior of users to foresee the intentions of attacking the system willingly or not;
- the directions to which the system evolves at a normal usage rate; how the input data given by users generates errors and what are the mechanisms through which these flaws in design can be eliminated;
- the behavior of security components to a series of sustained attacks on the system.

A set of indicators $CSI = \{CSI_1, CSI_2, \ldots, CSI_n\}$ are built, where *n* represents the total number of indicators that cover the requirements previously defined.

The *CSI* set is organized on three categories, so that each indicator can be assigned to one of the mentioned directions, as presented in Table 2.

Table 2. The indicators assignment matrix

CSI	Behavior		
	User	Security components	Application
CSI_1	1	0	0
CSI_2	0	0	1
...	...	...	...
CSI_i	0	1	0
...	...	...	...
CSI_n	0	0	1
	$UI = \sum_{i=1}^{n} CSI_i$	$SI = \sum_{i=1}^{n} CSI_i$	$AI = \sum_{i=1}^{n} CSI_i$

Based on the indicator assignment matrix the following measures are revealed with the restriction $UI + SI + AI = n$:

- UI is the number of indicators assigned in the category of user behavior measurements;

- SI is the total number of indicators that measure the security components reactions at frequent attacks;
- AI represents the number of indicators from the category which analyses the application's behavior based on the user inputs.

Several conditions must be met in order to have a set of unitary indicators, such as:

- the codomain must be between $[0; 1]$, each indicator that doesn't met this condition must suffer a normalization process, based on the following formula:

$$CSI_i^{new} = \frac{CSI_i^{old} - a}{b - a},$$

where:

CSI_i^{new} – the new value of the indicator in the $[0; 1]$ interval;

CSI_i^{new} – the old value in the $[a; b]$ interval;

a – the minimum value from the codomain;

b – the maximum value from the codomain.

- the indicator's lower value means a low quality characteristic and the opposite.

For achieving this homogeneity between the indicators from the *CSI* set, a unitary method in constructing them must be applied, consisting in the following steps:

P1. the set of collaborative security influence factors is defined;
P2. procedures for data acquisition regarding the collaborative security influence factors are developed;
P3. a database for storing these data systematically gather is constructed;
P4. analytical expression structures are generated;
P5. a set of performance criteria for the indicators is defined;
P6. based on the analytical expression structures and on the database filled with the measurements a software product estimates indicators coefficients;
P7. the performance level for each indicator is established for each performance criteria defined;
P8. the indicator with the best value for the set of performance criteria is chosen.

Let $CSI_i = \frac{x}{y}$, be the indicator associated with the *i* characteristic.

After, for each security characteristic, a suitable indicator has been determined for describing its behaviour, an analysis for testing the indicators' reliability is appropriate to be made by verifying their properties:

- sensitivity is the property that allow the indicator to adjust proportionally the output based on the input variations; if the *x* factor varies with δ, than the CSI_i indicator varies with $\frac{\delta}{y}$:

$$CSI_i' = \frac{x + \delta}{y} = \frac{x}{y} + \frac{\delta}{y} = CSI_i + \frac{\delta}{y}$$

- non-compensatory gives the indicator the ability to determine different variations for different input factors; if both *x*, *y* factors are multiplied by δ, than the CSI_i indicator doesn't varies at all, meaning that the indicator is compensatory:

$$CSI_i' = \frac{\delta \cdot x}{\delta \cdot y} = \frac{x}{y} = CSI_i$$

- non-catastrophic represents the capacity of an indicator to determine an output value in any situation, no matter what the input factors take values; for an absent *y* factor of which value is zero, the value of the indicator cannot be determined.

After each indicator is built and tested for its properties, they can be aggregated into a single metric to synthesize better the system's characteristics.

4 Ways to increase collaborative informatics security

In order to determine ways to increase the security, on start from the requirements which must be full filled in order that security gain a collaborative aspect and by analyzing ways to increase the concern:

- development of new tools;
- risks management;
- increasing complexity of informatics applications;
- increasing diversity of users, attackers, operators, administrators, developers.

In the context of so many resources associated to so many risks a question arises regarding the optimization of the entire system in such a way that:

- a resource isn't used more than a predefined limit;
- all security resources are assigned;

- the necessary of resources for each security risk NSR_j, $j = \overline{1,m}$ must be covered;
- the costs of collaborative system security risks must be minimized.

Each resource, $R_i, i = \overline{1,n}$, has a limited amount, $b_i, i = \overline{1,n}$, used for treating the identified security risks.

Each security risk, $SR_j, j = \overline{1,m}$, has a cost associated, CSR_j, $j = \overline{1,m}$, which in case is not treated, partially or totally is inflicted into the collaborative system.

The optimization problem is defined as a minimization of the costs inflicted by a non-security scenario or by a partially security policy in which some security risks are treated and others not.

The minimization function is defined as:

$$\min \sum_{j=1}^{m} \frac{\left(NSR_j - \sum_{i=1}^{n} scm_{ij}\right)}{NSR_j} \cdot CSR_j$$

For solving the optimization problem, the following restrictions apply:

- $\sum_{j=1}^{m} scm_{ij} \leq b_i$, the amount of resources from *i* category must be lower or equal than the total amount of resources available from *i* category;
- $\sum_{i=1}^{n} scm_{ij} \leq NSR_j$, the amount of resources used must satisfy the necessity of resources required by the security risks from the *j* category.
- $scm_{ij} \geq 0, \forall i = \overline{1,n}, \forall j = \overline{1,m}$.

After finding the distribution of resources based on the minimization function and optimization restrictions, the indicator degree of coverage, IDC, is defined to calculate how much of the security risks were covered by resources:

$$IDC = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m} scm_{ij}}{\sum_{j=1}^{m} NSR_j}$$

The IDC indicator takes values between $[0; 1]$.

If IDC=0, no resources were used in controlling the collaborative system's security risks.

If IDC=1, the risks were completely eliminated by directing resources so that all necessary of resources for each security risk category was fulfilled.

Determining the amount of resources scm_{ij} from *i* category used in combating the security risks from *j* category, the collaboration between them is optimized, so improving the general level of security.

On a global scale collaborative systems are based on the Internet and they are using web applications in order to get the benefits of a technology that reached the maturity and is reliable enough to justify continuation of development.

Considering that global collaborative systems are based on web applications, in this case the informatics security comes to secure the web servers that are hosting the applications and the web browsers that are being used for accessing these web applications as well as the communication channels used between browsers and web servers. In the current conditions the collaboration over web platforms involves that each user, using a collaborative application, will have to identify itself by the means imposed by the provider controlling the application.

When creating an identity for accessing a collaborative web application it is said that one is creating an account. Usually a user will have many accounts for different web applications, with the possibility of using different credentials for accessing each of these accounts.

The process through which one will identify itself in front of a collaborative application it is called login process. Usually for non-critical applications, the login process is based on a user name and a password. It is highly recommended that for different web applications to use at least different log in passwords, otherwise a security issue in a weakly secured application will be transmitted to the other web applications that a user is constantly accessing.

Security issues in the login process consist in allowing brute force attacks as well as SQL injection attacks.

In order to prevent this kind of threats the login systems must validate the inputs coming from the users and lock the accounts in the case of a brute force attack detection or just block the entire requests in the case of a SQL injection attack detection.

For the applications storing personal information with the potential of generating important financial damages for a user, a flaw in the login process is critical, thereby most of these systems will use an identification process that is based on a user name and a one-time password generated by a hardware device that must be synchronized with the authentication module of the web application. This is one of the most secure login methods available at this moment, and its strength relies on the fact that

an attacker will need the hardware device for effectively gaining access to an account any time he wants.

5 Collaborative security in banking informatics systems

The collaborative banking systems that are knowledge-oriented and which are in current operation, needs to be redesigned in order to take the facilities offered by new technologies. In the banking informatics systems there are encountered very large databases, which are complete and correct. The use of data mining algorithms allows the extraction of relevant information and turns it into knowledge, used in the structure and classification of systems analysed.

Collaborative systems encountered in the banking field are very discussed and analysed, because they offer multiple collaboration possibilities. These ways to collaborate are analysed in followings directions:

- collaboration between banking departments;
- collaboration between informatics applications;
- collaboration between network branches.

The banking information system must be collaborative, because it requires the communication, coordination and cooperation of different informatics applications, in order to achieve a common goal.

The banking system is collaborative when the followings conditions are achieved:

- the informatics system is developed as collaborative system (1);
- the users works in a collaborative manner (2);
- the security is collaborative (3);
- the use of banking system is as collaborative system (4).

Figure 4 presents the influence of the four conditions in order to consider that the banking system is designed to be collaborative.

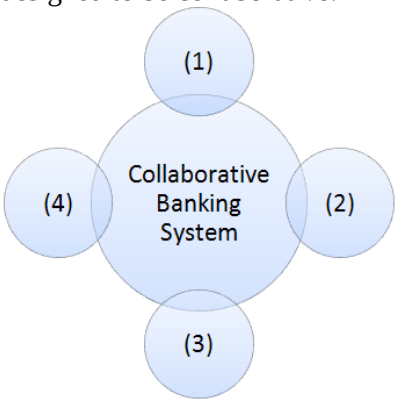

Fig. 4. Collaborative banking system

In banking information systems, the new security elements that must be taken into consideration in the case of banking applications are not related to users' access, because this was already solved. The future attacks will be provided by existing users and customers, which will exploit security vulnerabilities of the applications, after they are logged in. These vulnerabilities refer to the possibility to execute payments from an unauthorized account or in the name of another user or customer. Taking into consideration that payments are made electronically and in real time, these situations are identified when is too late. The reality gave us different cases when such situations were happened and some banks had significant losses [5].

If an incorrect transaction on a client account is made, meaning that it has made a payment to another beneficiary than the correct one or it transferred a wrong amount of money, then the payment reversal is carried out and a new transaction account is registered. Once registered a transaction on an account, it is no longer clear. The payment reversal requires crediting the customer's account with the equivalent payment, a situation which leads to two entries in the database, the one related to the payment and other related to the payment reversal. This working method has advantages such as keeping track of all transactions carried out on an account. Informations regarding banking transactions are increasing their value as aging. Banks realized this opportunity and charges for the availability of the old customer transactions for an account. If a customer requires a proof of one payment from his account, and the payment was made three years ago, the bank offer the customer acount statement for the required payment day for a fee.

When a customer requests preferential discounts and commissions for conducting operations, the bank analyzes the history of the customer transactions and the monthly transactions volume. The bank has all the transactions made by all the customers in a long period of time. If one bank has N branches and each branch makes an average of K daily transactions, then in H days, the total number of transactions $NTR=N*K*H$ represents hundreds of millions. With complete databases related to all transactions conducted by all customers, the bank examines the customer's money turnover and decides whether to grant preferential discounts and commissions.

The problem is to develop processes to search the database for a truncated key.

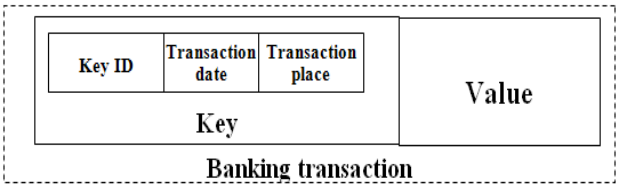

Fig. 5. Banking transaction elements

All the customer's transactions for a certain value are extracted if it's preferentiabily requires.

The main feature of a modern banking informatics system is the connectivity level between the elements involved in the banking activity. The collaborative banking system is a system with high complexity, with a large number of components and a large variety of links between them.

In the case of a banking informatics system, *BIS*, let's consider that three of four conditions are achieved in order to become a collaborative system, namely (1), (2) and (4). In this situation, the system was developed to be collaborative, the users interact in a collaborative way and the use of system is as a collaborative system. In order to become a full collaborative banking system, *CBS*, the third condition must be also respected, namely the security must be collaborative.

In Table 3 is presented a relation between the banking system and the conditions that must be respected in order to be declared collaborative system.

Table 3. Differences between *BIS* and *CBS*

	Cond. (1)	Cond. (2)	Cond. (3)	Cond. (4)	Colla-borative
Banking Informatics System (BIS)	Yes	Yes	No	Yes	No
Collaborative Banking System (CBS)	Yes	Yes	Yes	Yes	Yes

Informatics systems from the banking field differ one from each other by security of their components. In order to evaluate the degree in which the security is collaborative for each system, indicators are built and the systems are ranked based on these indicators.

All the informatics applications developed in a bank must meet the security and interoperability characteristics in order to be integrated [13] in the banking informatics system and to work collaboratively.

6 Security inside grid computing architecture

The concept of grid computing refers to a collaborative system of computers that cooperate to achieve a common objective, difficult to achieve with single resources [9], [10]. The computers network that form the grid computing [11] involves the geographical dispersion of computers, these being located in distant locations, distributed, such as the agents of a collaborative system.

In the banking field, the concept of grid computing is widely used, the banking informatics system being a collaborative system that requires the existence of many servers, distributed in different branches of a bank. Generation of complex reports in a bank branch, reports regarding the volume of payments made by a customer in a certain period, requires the access to various databases and processing the records in order to extract the transactions made by the specified customer. This processing is achieved in real-time, by collaboration of servers from the branch with those from bank headquarter, cooperation that is transparent at the level of informatics system users.

In a bank, millions of transactions per minute are executed [12], being received on different channels within the informatics system. There are customers who make payments via Internet banking and home banking services, other customers prefer to make them in the bank branch, and other customers through mobile banking. All these payments reach the same banking informatics system and are instantly processed with the help of computing power offered by the bank's server network. At the same time, in the informatics system enters other categories of transactions, such as receipts, settlement of promissory notes, foreign exchanges, POS transactions, that determine movements on customers' accounts and the use of hardware resources. The importance of real-time execution of these types of transactions is paramount. If a customer made an foreign exchange through internet banking, in order to credit an account in foreign currency, and immediately after the foreign exchange, he make a payment from the foreign currency account, through mobile banking, is very important the time when the foreign exchange was executed in order to not reject the payment from foreign currency account on grounds of insufficient funds. There are many cases in which the customers make foreign exchanges in the branch and they are late processed thanks to the human factor intervention.

Banks use grid computing also in the crediting process, in order to establish profiles of good payers and bad debtors' customers, in order to perceive loans fees, to determine the non-performing loans. Every night, the informatics system charges the loans fees and calculates penalties for debtors. Such processing is performed using a configuration of servers working in parallel.

Figure 6 shows the grid computing architecture of a banking informatics system, which includes the following application servers:

- Internet Banking Server;
- Domestic Payments Processing Server;
- Multicash Server;
- Loan Admin Server;
- Global Payments Processing Server;
- Websphere Portal Server;
- Intranet Server;
- Mail Server;
- Comprehensive Banking Server.

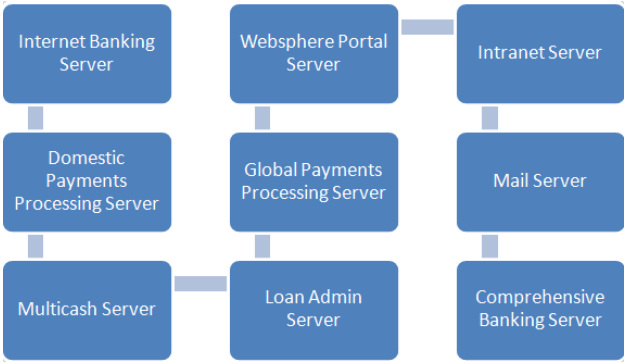

Fig. 6. The grid computing architecture of a banking informatics system

Each server has a well-defined role within the bank's informatics system. When the processing power of a server is exceeded, additional resources are automatically allocated from the other servers on the network that are not involved in processing at that time.

The advantages of grid computing architecture is given by the increasing processing power and improved capabilities of the applications running in the banking informatics system. In a classical architecture, when an application needs supplementary resources to complete a task, it will not receive these resources, even that they are available.

Daily transactions that take place in a bank conduct to generate very large data sets. When making a transfer between two accounts opened at the same bank, in the bank's informatics system two processing are performed, respectively one for debiting the payer account and the other for crediting the beneficiary account. Collaborative models for accomplishing the operations with very large data sets, via grid computing, aimed parallel processing on different servers and the existence of intelligent agents that prioritizes the operations and establish the order of transactions execution from processing queues. If a customer makes a transfer from the account A to the account B, and from account B makes a payment in the account C, both transactions are sent to be processed in the same package and at the same time. The informatics system will process first the transfer from account A into account B, and then the payment from account B to account C. If in the account A are insufficient funds, the two transfers are moved to a reprocessing queue. At reprocessing, the informatics system will apply the same priority of operations execution, so that both to be successfully executed.

The evolution of distributed systems and the grid computing impact on the nature of realized processing are the starting points in developing a new category of informatics systems with collaborative character and with a high level of security [14] [15] [16].

7 Conclusions

Collaborative informatics security is a new concept and gives a new perspective on the informatics security of distributed systems. It combines the key elements of collaborative systems and informatics security to provide strong security capabilities in order to prevent attacks and eliminate vulnerabilities.

Computer networks have significantly contributed to the development of Internet and web applications. The complex web applications, such as those that allow the generation of maps in real time, in a collaborative environment, they need numerous hardware resources to run timely and to better respond to user needs. Some applications use both the processing power of the server on which are installed, but also of the client from which are accessed.

For improving the model of distributed systems that are being used in a modern knowledge-based society, it is important for the systems to be fault tolerant, it is important to increase the rate of availability and to reduce the situations where resources are unavailable and also information security for the components in the system plays an important role in this situation.

References:

[1] A. W.M. Smeulders, W.Bouten, A. H.C. van Kampen, *E-Science research focus FNWI*, Universiteit van Amsterdam, 2009.

[2] Moore, Cramming more components onto integrated circuits, *Electronics Magazine*, 19 April 1965.

[3] K. Bettina, The sociological perspective on the knowledge-based society: assumptions, facts and visions, *Munich Personal RePEc Archive*, February 2008.

[4] F. Jörg., P. Ulrike, G. Stavros, New Forms of Work Organisation and Flexibility in the Knowledge-based society, in: Huws URSULA. (ed.): *The Transformation of Work in a Global Economy: towards a conceptual framework*, Leuven, 2006, pp. 45-60.

[5] I. Ivan, C. Ciurea, Security of Collaborative Banking Systems, *Proceedings of the 4th International Conference on Security for Information Technology and Communications, SECITC'11*, November 17-18, 2011, Bucharest, Romania.

[6] P. Pocatilu, M. Doinea, C. Ciurea, Development of Distributed Mobile Learning Systems, *The 9th WSEAS International Conference on Circuits, Systems, Electronics, Control & Signal Processing (CSECS '10)*, Vouliagmeni, Athens, Greece, December 29-31, 2010, pp. 196-201.

[7] J. Wu, *Distributed systems design*, CRC Press, 1999, ISBN 0-8493-3178-1.

[8] Web,http://www.esecuritytogo.com/ccpage.aspx?pageid=7&lid=11&lgid=1&name=Network+Risk+Assessment, Available for download on February 21, 2012.

[9] M. Ong, M. Alkarouri, X. Ren, G. Allan, V. Kadirkamanathan, H. A. Thompson, P. J. Fleming, Grid-based decision support with pro-active mobile computing, *2005 IEEE International Conference on Services Computing*, 11-15 July 2005, Vol. 2, pp. 59-66.

[10] I. Kafeza, E. Kafeza, C. Coutras, Legal issues in grid collaborative environments, *International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2007. CollaborateCom 2007*, 12-15 Nov. 2007, New York, NY, pp. 72-77.

[11] Xuebin Chen, Guolin Duan, Yan Sun, Jiantao Gu, Research on Key Technologies for Grid-Based Network Collaborative Design, *Fourth International Conference on Networked Computing and Advanced Information Management, 2008. NCM '08*, 2-4 Sept. 2008, Gyeongju, Vol. 2, pp. 639-644.

[12] I. Ivan, C. Ciurea, S. Pavel, M. Doinea, Security of Collaborative Processes in Large Data Sets Applications, *Proceedings of the 5th International Conference on Applied Statistics*, November 19-20, 2010, NIS Publishing House, Bucharest, Romania, ISSN 2069-2498.

[13] M. Kasem, N. Chahin, A Novel Approach for Meeting the Challenges of the Integrated Security Systems, *WSEAS TRANSACTIONS on SYSTEMS*, Issue 9, Volume 10, September 2011, ISSN 1109-2777, pp. 281-294.

[14] M. Muntean, Collaborative Environments in the Global Economy. Considerations Concerning Some Collaborative Systems, *Recent Advances in Computer Engineering Book – Proceedings of the 2nd World Multiconference on Applied Economics, Business and Development*, Tunisia, pp. 60-64, 2010, ISSN 1790-5109, ISBN 978-960-474-184-7.

[15] J. N. Sheen, Information Security Investment Decision-making based on Fuzzy Economics, *WSEAS TRANSACTIONS on SYSTEMS*, Issue 6, Volume 9, June 2010, ISSN 1109-2777, pp. 669-678.

[16] R. Pirinen, J. Rajamäki, L. Aunimo, Rescuing of Intelligence and Electronic Security Core Applications (RIESCA), *WSEAS TRANSACTIONS on SYSTEMS*, Issue 10, Volume 7, October 2008, ISSN 1109-2777, pp. 1080-1091.