Distributed Computing and Artificial Intelligence, 11th International Conference
Distributed, Grid, Cloud and Mobile Computing

Exploring the Role of Macroeconomic Mechanisms in Voluntary Resource Provisioning in Community Network Clouds .................................................. 269
Amin M. Khan, Felix Freitag

Performance and Results of the Triple Buffering Built-In in a Raspberry PI to Optimize the Distribution of Information from a Smart Sensor ................. 279
José-Luis Jiménez-García, José-Luis Pozo-Luján, Juan-Luis Pesadas-Yagüe, David Baselga-Masía, José-Enrique Simó-Ten

Mobile Access to Sensor Network: A Use Case on Wildfire Monitoring .......................................................... 287
Sergio Trilles, Óscar Belmonte, Joaquín Huerta

Building Scalable View Module of Object-Oriented Database .......................................................... 295
Haeng-Kon Kim, Hyun Yeo

Bioinformatics, Biomedical Systems, E-health

E-Nose System by Using Neural Networks .................................................. 311
Sigeru Ono, Mitsuak Yano

Modelling an Orientation System Based on Speculative Computation .................................................. 319
João Ramos, Ken Satoh, Paulo Novais, José Neves

Stable Learning for Neural Network Tomography by Using Back Projected Image .................................................. 327
Masaru Teranishi, Keita Oka, Masahiro Arimoto

Security Considerations for Patient Telemonitoring Schemes through Wireless Networks .................................................. 335
V. Morales, D. Cortés, N. Gordillo, A. De la Torre, D. Aspeitia

Development of an Ontology for Supporting Diagnosis in Psychiatry .................................................. 343
Cátia Silva, Gerei Marreiros, Nuno Silva

Augmented Reality Sign Language Teaching Model for Deaf Children .................................................. 351
Jorge Jonathan Cadeñanes Garmica, Marla Angélica González Arrieta

A Multi-agent Simulation: The Case of Physical Activity and Childhood Obesity .................................................. 359
Rabia Aziza, Amel Borgi, Hayfa Zagaya, Benjamin Guinhouya

The Absorptive Capacity-Based View of Training: Enhancing Organizational Performance. An Exploratory Study in Spanish Family Businesses .................................................. 369
Felipe Hernández Perlines, María Yolanda Salinero Martín, Benito Yañez Araque

Data Mining, Information Extraction, Knowledge Representation

LIWC-Based Sentiment Analysis in Facebook Comments: Estimation of Words: emotionally Intensity, Articulation,..., and Intensity of Adjectives-Affecting-Level .................................................. 279
Estanislao López-López, María del Río Sánchez, Leticia Almela, Miguel Ángel Rodríguez, Geni Alor-Hernández

Data Extraction Tool to Analyse, Transform and Visualise Electricity Data ......... 287
Ino F. Pereira, Tiago M. Sousa, Isabel Correia, Tiago Pinto, Zita Vale, Hugo Morais

Are There Semantic Primes in Formal English? .................................................. 295
Johannes Fähndrich, Sebastian Altmüller, Thomas Hofmann

The Age of Confidentiality: A Review of Law, Policy, and Internet ......... 303
Antonio Juan Sánchez, Yves Demuynck

Extracting Sentences Describing Risks and Compromises from Biomedical Literature .................................................. 311
Tiago Nunes, Sérgio Matos, José Luís Silva

TKG: A Graph-Based Approach to Enriching Knowledge Graphs .................................................. 327
William Daniel Abilhoa, Leandro Nunes

Image Processing, Tracking, Robot Industrial Systems

Outdoor Robotic Companion Based on UWB, Radar and GPS Guidance .................................................. 335
Edward Crott, Dani Martinez, Javier Mora, Tomas Pallela, Davinia Font, Mercè Tani

A Threshold Scheme for 3D Objects Based on Position and Orientation ........................................................................ 343
Angel Martín del Rey

Generation Method of the Trigger Sign System to the Harmful Animals with Infrasound Technology .................................................. 359
Fumio Takeda

2-Scene Comic Creating System Based on Emotions .................................................. 369
Miki Ueno, Naoki Mori, Keinosuke Matsui

A Brief Approach to the Ear Recognition System .................................................. 377
Pedro Luis Galdámez, María Ángelica García, Miguel Ramón Ramón
Security Considerations for Patient Telemonitoring Schemes through Wireless Networks

V. Morales, D. Cortés, N. Górdillo, A. De la Torre, and D. Azpetia

University of Ciudad Juárez, Juárez, Chihuahua, México

Abstract. In this study, security aspects are considered for the protection of medical information in patient telemonitoring schemes. In order to propose mechanisms to efficiently protect clinical information, it is presented a case study of a wireless network telemonitoring scheme, the results of a risk assessment to detect security problems in this type of schemes are analyzed.

Keywords: Telemedicine, Telemonitoring, Clinical Information Security, Risk Assessment.

1 Introduction

There are diseases that require constant monitoring of patients that should remain hospitalized so that their biological parameters can be monitored until their health is stabilized or improved. However, in other cases it is not necessary for these patients to remain in the hospital because despite having a chronic illness, their health is not considered to be critical. In the list of the chronic diseases that require constant monitoring or surveillance are diabetes mellitus, cardiovascular diseases, lung diseases, among others. Recently, several studies [1-3] in the area of telemedicine dedicated to the care of patients whose health requires constant monitoring have been proposed. Remote monitoring or telemonitoring is an area of telemedicine in which, through various instruments, diverse biological parameters can be monitored in order to provide timely care in case an emergency situation arises with the patient. Usually these patients are in their own home, so the instruments used to perform remote monitoring should be accessible and easy to use.

Current technologies for patient telemonitoring involve transmission of data through network communications such as Internet, cellular networks, satellite, etc. These data include sensitive medical information that must be protected from tampering. This work presents different schemes and telemonitoring technologies and evaluates, through a risk assessment, the need to employ security mechanisms to guarantee that the information is complete and reliable. In Section 2 telemonitoring schemes proposed for various health areas are described. Section 3 analyzes the security aspects to be considered for the development of telemonitoring systems. In Section 4 a risk assessment process based on current technologies is conducted. Final conclusions are presented in Section 5.
2 Telemonitoring Schemes

Several biological parameters such as ECG, EEG, insulin level, blood pressure, oxygen saturation, among others can be monitored with biomedical technology available today. However, through a telemonitoring system, related events such as the patient’s symptoms or medications can also be recorded and transmitted. Due to the different ways of measuring or capturing clinical information of patients, two areas of remote monitoring can be defined:

- Automated telemonitoring. A biological parameter or event information is acquired through a device that is capable of automatically (or scheduled) transmit such information. This can be done in different ways:
  - Acquisition and transmission in specific periods. According to the need of monitoring the patient a time frame (e.g., every 4 hours) is specified so that the clinical information is acquired and immediately sent to a monitoring center through a telecommunications network.
  - Acquisition with no scheduled transmission. A time frame for the acquisition of information is specified, however, it will be transmitted to a monitoring center if one parameter is out of the specified limits or, when a particular event occurs.
  - Acquisition and transmission with alert. As in the first case, information transmission takes place after every acquisition. However, if any value is outside a specified limit or a specific event is present, an alert is generated and transmitted along with clinical information.

- Conducted telemonitoring. Sending clinical information to the monitoring center requires a transmission medium for example through a web application. This type of telemonitoring requires the intervention of the patient or another person, which can reduce its efficiency.

Making appropriate use of information and communication technologies, telemonitoring platforms can help to increase the quality of patient care reducing public expenditure on care and treatment. In recent years several telemonitoring schemes have been proposed as described in [4], [5], [6] and [7]. Having a particular common: the transmission technologies, they vary according to the services provided and the type of patients they treat.

Wireless communication networks offer additional advantages to remote patient monitoring. The patient can be monitored from anywhere with cellular or even satellite coverage. Moreover, not only the information is received and accessed from hospitals or monitoring centers, it can also go directly to relevant medical staff through common mobile devices like cell phones or tablets. A patient telemonitoring system can make use of common wireless communication standards, such as Bluetooth, WiFi or cell phone technologies.

2.1 Case Study: A Wireless Network Telemonitoring Scheme

Figure 1 briefly describes a telemonitoring scheme of diabetic patients developed at the University of Ciudad Juárez. This scheme will serve as a basis for making a risk assessment to detect security problems in telemonitoring systems.
G, EEG, insulin level, blood pressure, monitored with biomedical technology monitoring system, related events such as can also be recorded and transmitting or capturing clinical information of can be defined:

critical parameter or event information is able of automatically (or scheduled) be done in different ways:
specific periods. According to the need frame (e.g., every 4 hours) is specified a acquired and immediately sent to a communications network.

transmission. A time frame for the ac-
ded, however, it will be transmitted to a

alert. As in the first case, information acquisition. However, if any value is for event is present, an alert is generated clinical information to the monitoring for example through a web applica-

is the intervention of the patient or

and communication technologies, tele-

the quality of patient care reducing in recent years several telemonitoring [4], [5], [6] and [7]. Having a partic-

eto vary according to the service.

additional advantages to remote pa-

information is received and ac-

it can also go directly to relevant devices like cell phones or tablets. A panel of common wireless communication phone technologies.

1. Telemonitoring Scheme

Scheme of diabetic patients developed scheme will serve as a basis for making in telemonitoring systems.

Fig. 1. Components of the case study telemonitoring scheme

The scheme makes use of wireless communication networks, and is composed of the following environments:

- Patient environment. The patient or family performs the tasks of clinical information record from their own home or anywhere else they are. The patient has a commercial glucometer with the ability of transmitting information through Bluetooth. The glucose measurement is transmitted to a mobile phone with an Android native application that receives and retransmits information through a cell network to a database. The application also has the ability to receive information from the monitoring center or the physician in charge.

- Monitoring center. The monitoring center displays patient records through a web application. A list of patients and their most recent measurements is displayed, alerts are also displayed when measurements are considered outside the normal range.

- Medical environment. Consists of mobile applications for multiple platforms (iOS, BB OS, Android) used by physicians who have diabetic patients. Through the application the physician can check the records of glucose levels. The doctor also receives alerts and is able to send recommendations to patients, among other features.

3 Security of Clinical Information

A very important issue is maintaining clinical information safe. We call clinical information to all patient information which is of interest to the physician
(e.g. biological parameters, symptoms or events, medical imaging, medication information, lab results). Clinical information should be treated carefully in each of the telemonitoring environments to meet different security objectives [8]. These objectives are: authentication (identifying the client), confidentiality (only authorized can access the information), integrity (the information has not been transformed during the processing, transport or storage), availability (to have the information when needed), and audit (to track the accesses made to the information and the operations performed on it).

In most countries clinical information is considered confidential and can only be accessed by authorized clinicians. In telemonitoring schemes, clinical information is generated in the patient environment and is generally transmitted through public means of communication such as Internet, wireless networks, etc., which increases the possibility of unauthorized access [9, 10], and causes the need to include high security checks in the monitoring scheme [8–11]. More important is the data integrity, an alteration in the clinical information could lead to an action that threatens the patient's health. For example, in the scheme described in Fig. 1, suppose that in patient records the glucose value is 130 mg/dL (considered normal) and during the transmission the value is modified and instead the physician receives a value of 330 mg/dL (considered very high value), the doctor could immediately prescribe the increment of the insulin dose to regulate the glucose level. The patient then follows the instruction and the natural consequence would be that the glucose level decreases considerably, producing severe hypoglycemia. Wireless communications can present serious deficiencies to keep information secure, even if the communication protocols implement their own security mechanisms, they do not prevent some types of attacks.

4 Risk Assessment for Telemonitoring Schemes

In order to accomplish the risk assessment, the methodology proposed by NIST [12] was implemented. This methodology was chosen because of its particular focus on information systems, as well as considering the risk analysis systems in its early phases like the requirements analysis. This methodology is summarized in the following steps: system characterization, threat identification, vulnerability identification, control analysis, likelihood determination, impact analysis, risk determination, control recommendations, and results documentation.

The process is performed separately for each of the three environments, the way the specific risks to each environment could be identified. In the patient environment is assumed that the glucometer has been tested and used for commercial purposes and therefore performs the measurements correctly. As observed in Tab. 1, the highest risk comes from an internal attacker (someone with access to the devices) that can access the application to cause damage. In Tab. 2, the risks associated with the medical environment are very similar to those of the patient environment. The results of the risk assessment in the monitoring center are presented in Tab. 3. Within this environment we considered the web application, the database that concentrates information from all applications as well as physical infrastructure and telecommunications.

| Table 1. Results of the risk assessment |
|---|---|---|
| Threat | Action | Motivation |
| External | Intercepting and manipulating glucose values | Fun |
| Internal | Access the application | Cause damage/ delete or manipulate information |
| Patient or User | None | |

| Table 2. Results of the risk assessment |
|---|---|---|
| Threat | Action | Motivation |
| External | Remove or manipulate records | Fun/ damage |
| Internal | Access the application | Cause damage/ delete or manipulate information |
| User | Lost | None |

In all cases, special emphasis should be given to high level risks. Using access control to ensure authorized users and devices in the telemonitoring protocols will maintain information integrity. The selection and implementation of the telemonitoring scheme (hardware and software) must ensure operation or lack of response from any user. To achieve the desired availability...
or events, medical imaging, medication ingestion should be treated carefully in each of the different security objectives [8]. These objectives are: confidentiality (only when the client knows), integrity (the information has not been altered or modified), availability (to support and audit), and trust (to track the accesses made to the device).

In a telemonitoring scheme, clinical information collected is considered confidential and can only be used for the purpose of monitoring the patient's health. This information is transmitted through the Internet or wireless networks, etc., which are considered to have access [9, 10], and causes the need for monitoring schemes [8–11]. More important, however, is the fact that the clinical information could be used for other purposes. For example, in the scheme described above, the glucose value is 130 mg/dL (considered very high), the incremental dose of the insulin dose to regulate the instruction and the natural consequence is that severe hypoglycemia can cause serious deficiencies in the patient's health.

Security Considerations for Patient Telemonitoring Schemes

The methodology proposed by NIST was chosen because of its particular focus on telemonitoring schemes. The methodology is summarized in the following diagram: threat identification, vulnerability assessment, risk determination, impact analysis, results documentation, and risk management. For each of the three environments, the client could be identified. In the patient centric environment has been tested and used for collecting and analyzing the measurements correctly. As observed in an internal attacker (someone with knowledge of the application) is able to cause damage. In the clinical environment, the results of the risk assessment in the monitoring scheme are very similar to those of the risk assessment in the monitoring scheme. In this environment, we considered that the telemonitoring system transmits information from all applications over the telecommunications.

Table 1. Results of the risk assessment in the patient environment

<table>
<thead>
<tr>
<th>Threat</th>
<th>Action</th>
<th>Motivation</th>
<th>Vulnerability</th>
<th>Risk Probability</th>
<th>Impact Risk level</th>
</tr>
</thead>
<tbody>
<tr>
<td>External</td>
<td>Intercepting</td>
<td>Fun</td>
<td>Insecure</td>
<td>Yes</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>and</td>
<td>and</td>
<td>Cellular</td>
<td></td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>manipulating</td>
<td>glucose</td>
<td>network</td>
<td></td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>value</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Stolen phone</td>
<td>Economic</td>
<td>Patient</td>
<td>Yes</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>neglect</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>Internal</td>
<td>Access the</td>
<td>Cause damage</td>
<td>Weak or no</td>
<td>Yes</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>application</td>
<td>delete or</td>
<td>user access</td>
<td></td>
<td>High</td>
</tr>
<tr>
<td></td>
<td></td>
<td>manipulate</td>
<td>control</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sensitive</td>
<td>Yes</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>material</td>
<td></td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Medium</td>
</tr>
<tr>
<td>Damaging</td>
<td>Phone</td>
<td>Cause damage</td>
<td>User</td>
<td>Yes</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>Lost</td>
<td></td>
<td>distracted</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Wrong</td>
<td>None</td>
<td>Neglect</td>
<td>Yes</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>message</td>
<td></td>
<td>Physician</td>
<td></td>
<td>High</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>poorly</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>designed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>application</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2. Results of the risk assessment in the monitoring center

<table>
<thead>
<tr>
<th>Threat</th>
<th>Action</th>
<th>Motivation</th>
<th>Vulnerability</th>
<th>Risk Probability</th>
<th>Impact Risk level</th>
</tr>
</thead>
<tbody>
<tr>
<td>External</td>
<td>Remove or</td>
<td>Fun /</td>
<td>Insecure</td>
<td>Yes</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>manipulate</td>
<td>damage</td>
<td>Cellular</td>
<td></td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>records</td>
<td></td>
<td>network</td>
<td></td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>Stolen phone</td>
<td>Economic</td>
<td>Medical</td>
<td>Yes</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>neglect</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>Internal</td>
<td>Access the</td>
<td>Cause damage</td>
<td>Weak or no</td>
<td>Yes</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>application</td>
<td>delete or</td>
<td>user access</td>
<td></td>
<td>High</td>
</tr>
<tr>
<td></td>
<td></td>
<td>manipulate</td>
<td>control</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sensitive</td>
<td>Yes</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>material</td>
<td></td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Medium</td>
</tr>
<tr>
<td>Damaging</td>
<td>Phone</td>
<td>Cause damage</td>
<td>User</td>
<td>Yes</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>Lost</td>
<td></td>
<td>distracted</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Wrong</td>
<td>None</td>
<td>Neglect</td>
<td>Yes</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>message</td>
<td></td>
<td>Physician</td>
<td></td>
<td>High</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>poorly</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>designed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>application</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In all cases, special emphasis should be given to mechanisms that mitigate high level risks. Using access control techniques facilitates the intervention of unauthorized users and devices in the scheme. Proper implementation of cryptographic protocols will maintain the information protected against tampering and unauthorized queries. The selection and implementation of these protocols depend on the communication technology used. The elements used in the monitoring scheme (hardware and software) must have high availability as improper or lack of response from any of them could lead to a critical situation. To achieve the desired availability, the communication devices and means...
Table 3. Results of the risk assessment in the medical environment

<table>
<thead>
<tr>
<th>Threat</th>
<th>Action</th>
<th>Motivation</th>
<th>Vulnerability</th>
<th>Risk Probability</th>
<th>Impact</th>
<th>Risk level</th>
</tr>
</thead>
<tbody>
<tr>
<td>External</td>
<td>Remove /manipulate</td>
<td>Fun /damage /economic</td>
<td>Inadequate access controls</td>
<td>Yes</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>records</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal</td>
<td>Remove /manipulate</td>
<td>Damage /economic</td>
<td>Inadequate access controls</td>
<td>Yes</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>records</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Damaging</td>
<td>Equipment failure</td>
<td>Fun /revenge</td>
<td>Sensitive material</td>
<td>Yes</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Technique</td>
<td>Power failure</td>
<td>None</td>
<td>Bad maintenance</td>
<td>Yes</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Natural</td>
<td>Lost connection</td>
<td>None</td>
<td>None</td>
<td>Yes</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Fire</td>
<td>None</td>
<td>Sensitive material</td>
<td>Yes</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Flood</td>
<td>None</td>
<td>Location</td>
<td>Yes</td>
<td>Medium</td>
<td>High</td>
</tr>
</tbody>
</table>

of transmission used should be carefully assessed. In addition, each of the elements of the scheme shall maintain a unmanipulable record of each of the actions taken, thus tampering can be detected and in some cases prevented.

5 Conclusions

Telemonitoring schemes have significant advantages primarily oriented to the welfare of the patient; they also contribute in reducing costs to health institutions as they avoid some of the major complications in the patients health. The security of clinical information should be paramount part in the design of patient telemonitoring schemes, mainly due to the sensitive nature of this information and the implications arising from unauthorized access or alteration. The main objective of the work presented is to get and analyze the results of a risk assessment for a telemonitoring scheme. A case study was used in order to determine general issues for this kind of telemedicine schemes, so that any scheme with similar characteristics can be designed taking into account the results of this risk assessment. It allows to clearly visualize where to focus efforts to implement security mechanisms in telemonitoring schemes. The case study largely reflects recent telemonitoring proposals, so the results of the risk assessment here presented can be considered for telemonitoring schemes in general, and especially those using wireless communications. However, according to the particularities of each scheme, it is recommended to implement the risk assessment to consider all situations in which patient information is at risk.

References

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Risk Probability</th>
<th>Impact</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Yes</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Yes</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Yes</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Yes</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Yes</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Yes</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
</tr>
</tbody>
</table>

In addition, each of the elements is assessed. In addition, each of the elements has a manipulable record of each of the actions performed, and in some cases prevents the actions from being taken.

Advantages primarily oriented to the area in reducing costs to health institutions with the patients' health. The paramount part in the design of patient-centered electronic medical records of this information is authorized access to the system. The main point of this study was to determine whether the scheme, so that any scheme with a high impact can be adapted. The case study largely reflects the results of the risk assessment here presented schemes in general, and especially because, according to the particularities of each scheme, the risk assessment to consider each scheme is at risk.

References

Distributed Computing and Artificial Intelligence,
11th International Conference

The 11th International Symposium on Distributed Computing and Artificial Intelligence 2014 (DCAI 2014) is a forum to present applications of innovative techniques for studying and solving complex problems. The exchange of ideas between scientists and technicians from both the academic and industrial sector is essential to facilitate the development of systems that can meet the everincreasing demands of today’s society. The present edition brings together past experience, current work and promising future trends associated with distributed computing, artificial intelligence and their application in order to provide efficient solutions to real problems.

This year’s technical program presents both high quality and diversity, with contributions in well-established and evolving areas of research (Algeria, Brazil, China, Croatia, Czech Republic, Denmark, France, Germany, Ireland, Italy, Japan, Malaysia, Mexico, Poland, Portugal, Republic of Korea, Spain, Taiwan, Tunisia, Ukraine, United Kingdom), representing a truly "wide area network" of research activity. DCAI 14 Special Sessions have been a very useful tool in order to complement the regular program with new or emerging topics of particular interest to the participating community. Special Sessions that emphasize on multi-disciplinary and transversal aspects, such as AI-driven methods for Multimodal Networks and Processes Modeling and Multi-Agents Macroeconomics have been especially encouraged and welcome.

This symposium is organized by the Bioinformatics, Intelligent System and Educational Technology Research Group (http://biste.usal.es/) of the University of Salamanca. The present edition was held in Salamanca, Spain, from 4th to 6th June 2014.