BULETINUL INSTITUTULUI POLITEHNIC DIN IAŞI
Publicat de
Universitatea Tehnică „Gheorghe Asachi" din Iaşi
Tomul LVII (LXI), Fasc. 4, 2011
Secţia
ELECTROTEHNICĂ. ENERGETICĂ. ELECTRONICĂ

DATABASE SECURITY ON REMOTE PATIENT MONITORING SYSTEM

BY

ANAMARIA HARITON [*], MIHAI CREŢU, LUCIAN NIŢĂ and MONICA SĂLCIANU

"Gheorghe Asachi" Technical University of Iaşi,
Faculty of Electrical Engineering, Energetics
and Applied Informatics

Received, March 6, 2011
Accepted for publication: June 16, 2011

Abstract. A telemonitoring system aiming to collect and transmit essential patient health state data to a supervisor physician is proposed. The patient health state is measured by means of several dedicated wireless sensors, which values are saved into a local database. All new values that the local database stores in are periodically sent to the physician server and displayed into a graphical manner. Main objective of this remote monitoring system is to save and secure all useful information and personal information called confidential data. Database security and database synchronization ensure the performance of telemonitoring systems and this research aims to improve it.

Key words: wireless sensors; local database; remote monitoring system; patient health state.

1. Introduction

The alarming increase in the amount of population suffering from chronic diseases in modern societies (Lopez-Garcia *et al.*, 2010), has totally changed the healthcare panorama. Home telemonitoring has proved beneficial to both

[*] Corresponding author: *e-mail*: ahariton@ee.tuiasi.ro

institutions and patients avoiding unnecessary visits and even providing a motivation for patients to adhere to better health habits (Johnson *et al*., 2008).

Hospitalization is a very expensive and resource consuming alternative for those patients that have to be continuously monitored. This might be the case of different chronic diseases, when the illness is not so fast progressing, but on the other hand it is very important to continuously monitor the most important vital signs evolution in order to foresee a major complication of the illness or the case of old people monitoring: nowadays, there is a lack of time and energy to take care on old people by its family members. Besides some modern automated equipment that may help them, a monitoring system may help by instantly providing their physician with its vital parameters information and may raise an alarm if something goes wrong.

1.1. Database Security

With increasingly sophisticated attacks and rising internal data theft, database security merits a stronger focus that goes beyond traditional authentication, authorization, and access control (AAA).

Database security is the last line of defense, so it deserves greater focus on the protection of private data from both internal and external attacks than IT "pros" have traditionally given it[1]. Database security professionals and information security and risk management professionals crafting a security strategy should: align database security policies with information security policies, ensure well-defined and formalized database security procedures, enforce role separation and apply advanced security measures such as database auditing, monitoring, database encryption, data masking, and vulnerability assessment to all critical databases that store private data.

A study conducted from December 2000 until November 2006 shows that the number of security flaws in the Oracle and Microsoft database servers that have been discovered and fixed is lower for Microsoft database servers. The graphs with flaws that have been discovered by external security researchers in both vendors' flagship database products – namely Oracle 10g Release 2 and SQL (Structured Query Language) Server 2005 – point out that no security flaws have been announced for SQL Server 2005.

Considering that Web environment is today an often attacks target, this patient remote monitoring system need to secure information flow transmitted over the Internet.

Recent survey by the Enterprise Strategy Group found that while 84% of enterprises believe their data is secured, 57% have been breached in the last 12 months.

Clearly, many organizations have a false sense of security. With over 222,000,000 records compromized in 2009 alone, data security must be a

[1] IT pros is a software program developed by Windows which can detect and prevent website vulne-rabilities and thwart attacks.

priority. But protecting databases is not easy.

When reviewing database security, it is crucial to concentrate on two areas: how well the system has been hardened, and how the data and database access is controlled. Most hackers target the data held in a database. Therefore the server, where the database resides, needs to be hardened and protected, both physically and logically. Ideally, the database will be on its own dedicated machine, but it should never reside on a public-facing server, such as a Web server. Naturally, all system and database program patches should be installed, and unnecessary features should be removed or disabled. Most database programs have several default accounts and passwords, all of which need to be changed.

One of the best ways to determine how well these hardening procedures have been implemented is to run the appropriate Center for Internet Security (CIS) Benchmarks and Scoring Tools against both the server OS (Operating System) and the database. The Benchmarks are best practice standards for security configurations that help to determine how your systems measure up. These Benchmarks and Scoring Tools are available for most OSes, Oracle and Microsoft's SQL Server databases and can be downloaded for free.

Any applications that connect to the database should use an encrypted link, even if the database resides in a controlled network. All data, including connection strings, should be encrypted using SSL (Secure Socket Layers) or SSH (Secure Shell), for example, to protect it during transit.

So, in order to encrypt the connection to the FTP (File Transfer Protocol) service, we can use SFTP (Secure FTP), as shown in Fig. 1. SFTP is actually part of the SSH Daemon and is an extension to the SSH 2 protocol.

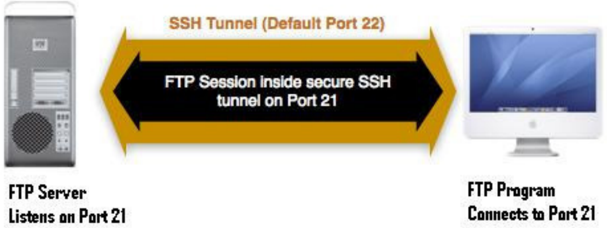

SSH Tunnel (Default Port 22)
FTP Session inside secure SSH tunnel on Port 21
FTP Server
Listens on Port 21
FTP Program
Connects to Port 21

Fig. 1 - Securing FTP with SSH.

SSH is perfect to keep confidentiality and integrity for data exchanged between two networks and systems. However, the main advantage is server authentication, through the use of public key cryptography.

Also, encrypted data should not store the encryption key on the database server. Applications and users that connect to the database should only have the minimum privileges required to complete their tasks, and access to system level resources should be controlled with Access Control Lists (ACL).

As far as protecting the database server from penetration, there should be a firewall protecting access to it and, if possible, the data supplied by the server should not be live production data. Production databases can be mirrored to separate servers so the Web server can provide access to the data without risk of contaminating production data (Cobb, 2008).

1.2. Organization of Telemonitoring System Applications

This paper proposed a new telemonitoring system, emphasizing on patient data acquisition and storing into a local database, data transmission and graphical presentation to the physician. Building a patient remote monitoring system requires intensive research and some important requirements are in terms of simplicity in use on a daily basis, agreeable user interface and accessible cost (Paré *et al.*, 2007).

The main goal the monitoring system has to comply with is to collect and transmit the patient data in such a way which doesn't disturb too much the patient. The physician has to be presented with essential and easy understandable graphical diagrams attempting to spare his data analysing time. Reliable data are provided at any time even if an Internet connection failure occurs sometimes or the clinician has closed the application. Once the physician reopens the application programme, he should be able to view all the monitored data for a selected patient and also to send back advises regarding his treatment.

The patient application should be intuitive, easy in use and simple enough to run it even on small hardware devices as mobile phones. It is highly probable that a person may not have a computer but a cell phone it's a usual personal device nowadays and it is important that the data collecting application runs even on these devices which doesn't allow large databases installation or other complex technologies.

2. System Methodology

2.1. Telemonitoring System Architecture

The data acquisition system comprises two separate applications which communicate one to another by means of an Internet connection (Fig. 2).

The patient application runs on a small device and its tasks are

a) to collect data provided by the vital signs sensors, to store the information into a local database;

b) to send the data to the physician computer whenever an Internet connection is available;

c) to receive and display the physician advice.

This application should perform some data processing in order to extract and display other informations regarding patient health state and has to transmit an SMS if the Internet connection breaks down and the patient needs the clinician attention and advice.

The patient application collects data from a list of vital signs sensors by means of a wireless connection.

The clinician application runs on the physician's laptop. It uses a large database which collects recorded data from many patients, filters the recorded data and graphically displays actual and historical for any required patient evolution data analysis. It also allows the physician to send back treatment advices to a selected patient.

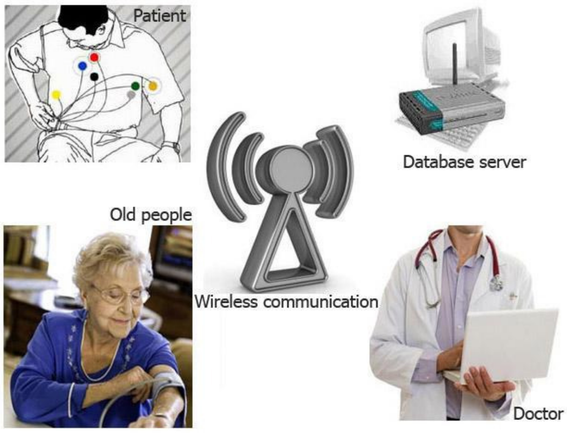


Fig. 2 – Patient health monitoring system architecture.

These two applications communicate each other through an Internet connection or by sending SMS's whenever an alarm, occurs.

The actual market offers a series of very small sized sensors which are easily connected to a patient body. Actually, an electronic chip includes several sensors measuring different patient body parameters as: temperature, heart rate, acceleration and/or electrocardiogram (Ultra Low Power..., 2010).

2.2. Technological Specifications of the Telemonitoring System

The steps which have to be pursued in order to provide the clinician application with reliable data related to the patient body monitored parameters are the following:

a) Measurement and display of the patient vital signs: related to the Bluetooth connections management and display of all notifications regarding the sensors status (connected/disconnected, battery low, required calibration etc.).

b) Saving all collected data and events into a local database: the database engine should be simple requiring a low consumption from the device battery or memory.

c) Synchronizing the local database with the clinician database: depending on Internet connection or device availability (On/Off); they are not connected all the time. We propose a solution to maintain these two databases synchronized even if the communication channel breaks down at a certain moment.

d) Building a graphical user interface for the clinician: it displays the current online measured data for a selected patient, processes the data and raises alarms related to the critical patient condition and sends physician advices back to the patient.

The patients have to be provided with simple enough and very clear notifications related to the sensors activity in order to initiate some actions aiming to maintain them working properly.

The SQLite database has been selected to save the data pertaining to this remote monitoring system. It is a free database, fast enough to satisfy the application needs and requires only 800 kB hard disk space. SQLite has attracted strongly the majority of developers for its advantages such as lightweight, easy to port, without copyright restrictions and so on. The data acquisition system has to be simple and efficient. It comprises two separate applications which communicate one to another by means of an Internet connection (Bi, 2009).

A service installed on the database server runs automatically anytime whenever the computer starts and it is responsible to answer to any patient devices requests. Once a new connection has been established, an algorithm decides which new data have to be transmitted, the amount of lost data since the last synchronization and options to recover it. Therefore, each database table line includes a flag informing if there are new recorded data or they have been already sent to the server.

The databases synchronization is performed by sending packages of multiple data lines and, if it breaks down, then all the data lines from a sending failure package still remain with the "new" flag marker. It is possible that only some data lines to be successfully updated on the server, but if the package sending fails, the "new" flag value is assigned to all the package data lines and there will be a new synchronization attempt. This seems to be a process that has to insert twice such data lines into the server database. Anyway, this effect is avoided by using a unique identifier for each data line and by defining a unique constraint on the server database.

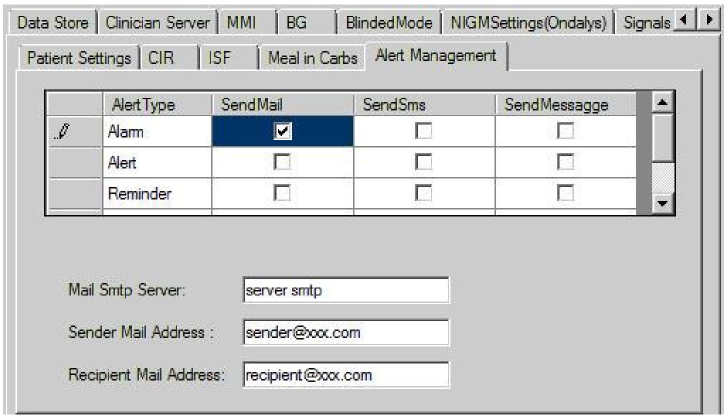
3. Conclusions

The telemonitoring system has been tested on several diabetic people during the clinical trials performed within the DIAdvisor FP7 research project. (DlAdvisor Project, 2010). The system uses a continuous blood glucose sensor providing real time data on the actual level of blood glucose and other few sensors which monitor the patient activity by measuring the acceleration and heart rate.

Based on these sensors measurements a prediction on the blood glucose level in the immediate future is raised and helps the patient to perform a specific action towards reducing the amplitude of the blood glucose modification.

The physician doesn't need to keep the application opened all the time.

The patient sensors data are received by a server which uses a large database and collect information from all registered patients. For the case when a patient needs medical attention due to a sudden critical condition and the physician application is closed, the patient application sends a SMS to the physician. For each type of critical condition which is possible to appear, the physician has the possibility to set the action to be performed by the system, using a separate configuration application (Fig. 3).



	AlertType	SendMail	SendSms	SendMessagge
✎	Alarm	☑	□	□
	Alert	□	□	□
	Reminder	□	□	□

Mail Smtp Server: server smtp

Sender Mail Address : sender@xxx.com

Recipient Mail Address: recipient@xxx.com

Fig. 3 – Configuration application.

Once the physician starts the application, then the programme connects to the database and reads all the available information related to a selected patient. This information includes

a) sensors values (temperature, blood glucose, heart rate) which characterize the patient health state;

b) events occurred during the monitoring time: hyper- or hypoglycaemia, high temperature, high heart rate;

c) devices status: sensors state, wireless connection, patient device status.

The physician has the possibility to send back to the patient observations or advices, helping him to correct the treatment.

Among the benefits of this system may by cited the followings:

a) an important economical impact over the healthcare system while the patient receives professional care ambulatory instead of consuming hospital funds due to hospitalization;

b) the patient may join his family earlier than in a common situation and still keeps the link with a physician by means of the monitoring system;

c) the system may benefit also the old people who are able to take care themselves, but need to evaluate their health state time to time by sending the recorded data to a physician database.

A patient needs only a cell phone with an installed Windows operating system and an Internet connection, and he will be provided with the monitoring device.

The major advantages and originality of the proposed telemonitoring system are the followings:

a) security and synchronization of local database with the clinician database;

b) it uses the newest user interface technologies (Windows Presentation Foundation, Windows Communication Foundation); the result is a robust and simply to use high quality graphical interfaces for the patient and clinician;

c) it solves all the problems related to a poor Internet connection quality (lost of data, database synchronization) which are inherent due to the ambulatory patient's treatment;

d) the system has been tested on diabetic patients and has proven its utility.

Acknowledgments. This work was financed and developed in the framework of the Project "EURODOC" (PhD scholarship ID 59410 OI POS DRU Ministry of Education, Research, Youth and Sports).

REFERENCES

Bi C., *Research and Application of SQLite Embedded Database Technology.* WSEAS Trans. on Comp., **8**, *1*, 83-92 (2009).

Cobb M., *How to Protect and Harden a Database Server.* Financial Services Information Security News, SearchFinancialSecurity.com., 2008.

López-García P., Bermúdez J., Illarramendi A., Berges I., *Customizin Home Tele-Monitoring Systems for Chronic Diseases.* Univ. of the Basque Country "P° Manuel de Lardizábal 1", San Sebastián, Spain, http://svn.plopez.info/website/publications/2010/eHealth2010a.pdf.

Paré G., Jaana M., Sicotte C., *Systematic Review of Home Telemonitoring for Chronic Diseases: The Evidence Base.* JAMIA – J. of the Amer. Med. Inform. Assoc., **14**, *3*, 269–277 (2007).

* * * *DIAdvisor Project.* http://www.diadvisor.eu, 2010.

* * * http://research.microscope.co.uk.

* * * http://www.appsecinc.com/products/dbprotect.

* * * http://www.cybercity.biz/tips/linux-unix-bsd-openssh-server-best-practices.html.

* * * http://www.databasesecurity.com/dbsec/comparison.pdf.

* * * http://www.saint-media.co.uk/2010/05/achieve-secure-ftp-sftp-with-dreamweaver-using-ssh-tunneling.

* * * *Ultra Low Power Intelligent Sensor Interface and Tranceiver Platform.* http://www.toumaz. com/public/page.php?page=sensium_intro, 2010.

SECURIZAREA BAZELOR DE DATE ÎNTR-UN SISTEM DE MONITORIZARE A PACIENȚILOR LA DISTANȚĂ

(Rezumat)

Sistemul de monitorizare la distanță a pacienților are scopul de a colecta şi de a transmite datele esențiale cu privire la starea de sănătate a pacientului către medicul supraveghetor. Starea de sănătate a pacientului este măsurată cu ajutorul unor senzori wireless ale căror valori sunt salvate într-o bază de date locală. Noile valori stocate în baza locală de date vor fi trimise periodic către serverul central al sistemului şi apoi afişate grafic. Principalul obiectiv al acestui sistem constă în salvarea şi securizarea informațiilor stocate în baza locală de date. Performanțele unui astfel de sistem de monitorizare sunt date de metodele de securizare şi de sincronizare a bazelor de date folosite iar prezenta lucrare îşi propune să îmbunătățească aceste metode.