Internet of Things in Healthcare : Interoperatibility and Security Issues

Liane Margarida Rockenbach Tarouco, Leandro Márcio Bertholdo, Lisandro Zambenedetti Granville, Lucas Mendes Ribeiro Arbiza, Felipe Carbone, Marcelo Marotta, José Jair Cardoso de Santanna
Institute of Informatics
Federal University of Rio Grande do Sul (UFRGS)
Porto Alegre, Brazil
liane@penta.ufrgs.br, berthold@penta.ufrgs.br, granville@inf.ufrgs.br, lucas@pop-rs.rnp.br, felipe.carbon@inf.ufrgs.br, mamarotta@inf.ufrgs.br, jjcsantana@inf.ufrgs.br

***Abstract*—Internet of Things devices being used now expose limitations that prevent their proper use in healthcare systems. Interoperability and security are especially impacted by such limitations. In this paper, we discuss today´s issues, including benefits and difficulties, as well as approaches to circumvent the problems of employing and integrating Internet of Things devices in healthcare systems. We present this discussion in the context of the REMOA project, which targets a solution for home care/telemonitoring for patients with chronic illnesses.**

Keywords-Internet of Things (IoT); Healthcare; Security

I. INTRODUCTION

Internet of Things (IoT) encompasses a set of technologies that enable a wide range of appliances, devices, and objects (or simply "things") to interact and communicate among themselves using networking technologies. Human beings supply most of the contents and information found on Internet so far, whereas in IoT, small devices are frequently the active element that provides the information. There are many applications for IoT; including healthcare systems, which are the main focus of this paper. Healthcare systems use a set of interconnected devices to create an IoT network devoted to healthcare assessment, including monitoring patients and automatically detecting situations where medical interventions are required.

It is generally recognized that the chronically ill, such as those with hearth failure, hypertension, respiratory diseases or diabetes require medical, hospital, and emergency services more often than regular patients [1]. Information and communication technologies are amongst the tools that could help mitigate some of the problems associated with aging populations, increased rates of chronic illnesses, and shortage of health professionals, and, at the same time, facilitate service reorganization. Modern measuring devices, such as, blood pressure, weight, and movement sensors, incorporate communication capabilities. They can create IoT networks implemented for home telemonitoring. These same devices are those usually employed by health workers to check the overall condition of patients with chronic illnesses.

REMOA[1] is a project which targets home solutions for care/telemonitoring of patients with chronic illnesses. Different strategies and protocols for general data exchange among monitoring devices like blood pressure monitors and movement sensors are considered. The project also encompasses the design and implementation of a healthcare-devoted middleware. The general system collects information from different sensing devices through a middleware that provides interoperability and security needed in the context of Internet of Things for healthcare. Monitoring devices are connected via wireless networking technology. The monitoring application frontend, which is functionally similar to a network manager, is responsible for storing, aggregating, consolidating, and comparing the collected information against historical series so that when thresholds are crossed, the frontend system may issue alerts or execute specific procedures. When limits are crossed, depending on threshold policies, alarms are triggered to enable health workers to promptly react to health-related events.

The topology of the typical home telemonitoring healthcare network includes an intermediary processing proxy that forwards sensing data to the remote server responsible for data analysis, consolidation, and critical events detection. In this way, surrounded by smarter environment that employs communication and information technologies, citizens (especially elders) and medical teams find better conditions to proceed with proper domestic-based treatments.

This paper is organized as follows: In Section 2 we list and describe the sensing devices being used. In Section 3 we present solutions to deal with interoperability issues in healthcare systems. In Section 4 we deal with security problems in telemonitoring healthcare systems, while in Section 5 we describe strategies and workarounds for solving current problems. Conclusions are presented in Section 6.

[1] REMOA: *Rede Cidadã de Monitoramento do Ambiente Baseado no Conceito de Internet das Coisas* (Citizen Network for Environment Monitoring Based on the Concept of Internet of Things).

II. DEVICES TO BE CONNECTED

Based on requirements of a home telemonitoring system for patients with chronic diseases (e.g., blood pressure, patient recovery of hospitalization), some devices have been selected (Figure 1) to be used in the REMOA project, in order to monitor some aspects of patients' health. These devices have Wi-Fi interfaces and features that enable interoperability and data transmission. Devices selected for use in the project are:

- A Panasonic BL-C230A Wi-Fi IP camera to detect the movements of monitored patients - The lack of movement in periods of the day when movements are expected may indicate some critical problem. The selected device is able to detect movements based on three different sources of data: 1) image; 2) sounds; and 3) body heat. Every movement detected sends forth an alert message that carries the images which are sent to an e-mail address or uploaded to an FTP (File Transport Protocol) server;
- A wireless body scale fitted with a Wi-Fi interface manufactured by Withings fitted with software which calculates the patients' percentage of fat, muscle mass, and body mass index. The standard configuration of this device connects the wireless network immediately after weighing and sends the data to an URL internally set to the manufacturer's website;
- A Withings blood pressure device with the peculiarity that its operation depends on the connection to an Apple device (iPad, iPhone. or iPod Touch). The operation is similar to the scale (both products are from the same manufacturer) with the difference that this device is operated via an application installed in an Apple device. The application is also responsible for sending measurement data to the remote server and informing the patient about the progress of the measurements, warning of possible errors in handling the device, such as poor posture or sudden movements that affect correct measurement of the patient's blood pressure.

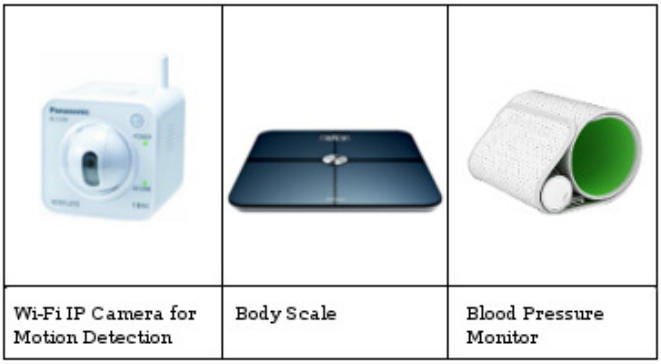

Figure 1. Devices being connected for home healthcare telemonitoring

The reading data sent from monitoring devices and patients' information will be accessed through a web browser on a regular computer and in Apps on smartphones and tablets. These devices are used by the medical staff to monitor patients' health and by patients who can access information about their own treatment and may interact with medical staff and other patients doing social networking and other activities typical of the context of Patient 2.0 where patients participate actively in their own treatment [2].

The device responsible for centralizing the data transmission of all selected device is a wireless Access Point (AP) that supports OpenWRT or DD-WRT. This approach enables the development and deployment of additional software, and supports protocols such as IPv4, IPv6, NAT, SNMP proxy and serves as a gateway to other monitoring devices.

III. INTEROPERABILITY ISSUES

The REMOA project was designed to deploy a monitoring environment based on Wi-Fi (802.11). At first, we expected that the various monitoring devices would be able to communicate with remote servers just through a Wi-Fi access point, which would serve as a gateway between Internet and our monitored environment. This approach, although applicable, has restricted the diversity of medical devices available, mainly because of the tendency to use Bluetooth technology in healthcare devices. This trend is due to the low cost and low power consumption of Bluetooth-enabled devices. Despite its major availability, we have only found a few solutions in the market which enable the interconnection between Bluetooth (802.14)/ZigBee (802.15.4) networks and Internet. This point was a challenging one adding difficulties in sending data collected by healthcare devices to a remote server over the network

In a fully Wi-Fi-based environment, the interoperability problem could be solved through a Wi-Fi/Bluetooth gateway, providing all management capabilities desired, either by using the Simple Network Management Protocol (SNMP) or Web services. However, even healthcare devices built with Wi-Fi interfaces aren't fully suitable for use in a flexible monitoring environment. We found that most of such devices operate by communicating with servers and proprietary system, as is the case of the Withings body scale. This problem required a circumvent solution to be implemented in the communication infrastructure. This workaround is centered in a Access Point (AP) running a Linux (OpenWRT / DD-WRT), and thus allowing the addition of the software to the AP. Although the transmitted data layout is proprietary, in most cases, like the Withings body scale, a traffic analysis revealed that the data is transmitted in plain text and using the JSON format, which represents a security weakness because it allows eavesdropping during the connection

IV. SECURITY ISSUES

The fact that personal private data will be collected through telemonitoring implies the need for strategies and mechanisms to ensure adequate security and privacy. As highlighted in [3], "having every 'thing' connected, new security and privacy problems arise, e.g., confidentiality, authenticity, and integrity of data sensed and exchanged by 'things'." This author lists the standard security requirements:

- Resilience to attacks - The system has to avoid single points of failure and should adjust itself to node failures;
- Data authentication - As a principle, retrieved addresses and object information must be authenticated;
- Access control - Information providers must be able to implement access control on the data provided;
- Client privacy - Measures need to be taken that only the information provider is able to infer from observing the use of the lookup system.

Nevertheless, in view of the mobility context where health agents will access patient's data when visiting their homes, it implies the need for "privacy enhancing technologies," as mentioned in [4], to ensure that the patient's personal data is protected against non-authorized access.

The solution for interoperability and management of home care network has been projected to use amplified network management concepts in order to include Internet of Things management separating the capabilities and functions of an object from the implementing technology such as RFID or WLAN as proposed in [5]. In this way, the management and security architectures must be oriented to monitoring events to ensure the security of medical devices and mobile devices and further use a unified authentication design for the whole set of systems, i.e., medical and infrastructures.

The planned authentication services use Shibboleth, a middleware layer for authentication and access control developed as an Internet2 project [6]. By using Shibboleth it is possible to take advantage of a Federated Authentication service already implanted by RNP (Rede Nacional de Ensino e Pesquisa - the Brazilian Research and Education Network). CAFe ("Comunidade Acadêmica Federada") , a federation of Brazilian research and education institutions acting as identity and service provider. CAFe allows every user to have just one user account in his/her origin institution that is valid for all services offered by the federation, thus eliminating the need of multiple passwords and multiple registration processes (Single Sign-On SSO). However, in the IoT context other security issues arise, to data integrity and user privacy because mobile devices are potential targets to malicious attacks, which requires further advancements in terms of studies and security countermeasures. In the case of healthcare environments, avoiding successful attacks to the system or at least mitigating them are primary goals because failures or information leaks can represent damages to the patients. In contrast to other domains that can absorb some costs of system abuse, healthcare systems cannot. Once sensitive information about an individual's health problems is uncovered and social damage is done, it is impossible to revoke the information [7].

Attackers have well defined goals when focusing on mobile devices. Usually, attacks aim at stealing users' information, attacking devices resources, or even shutting down some applications [8]. There are many threats surrounding mobile devices; the majority of these threats are inherited from conventional computing systems and adapted for mobile devices. However, some threats get more attention because of the potential problems they can cause to the systems. Examples of these threads are:

i) Man-in-the-Middle;

ii) Routing diversion attack;

iii) Denial of service aiming to cause a Battery Exhaustion in the device.

These attacks, when applied exclusively on mobile devices, expedite given factors such as: a) natural use of broadcast for communication; b) lack of certification sources; c) use of batteries as power source; and d) mobility. Therefore, to manage such a large range of mobile devices mapping and mitigating the most relevant threads in a given context is an essential task.

In this context, devices that operate in an wake-up and input data approach, as the Withings Body Scale used in this project, are less vulnerable to battery exhaustion attacks because the exposure time boils down a few seconds in which the device is connected through Wi-Fi interfaces and there is no service to be attacked. Moreover, interception and connection issues persist and the lack of any server/service authentication infrastructure to where the data will be sent and the lack of obscurity of content are security gaps that demanded a circumvent solution in the REMOA project.

V. CIRCUMVENT APPROACH

Given the problems described in the previous section, adjustments became necessary in the communication infrastructure initially planned, in order to enable using the concept of homecare IoT with a safer approach. In REMOA, an access point is used to provide several features and additional security functions (Figure 2):

i) A gateway connecting the devices BT / ZigBee to the Internet with encryption;

ii) Transparent HTTP proxy, to manipulate the transient data and account information from cloud IoT to Internet;

iii) IoT device management;

iv) Authorization, Authentication and Accounting for Internet access and systems used by patient and health agents.

The role of the gateway is to translate messages from one technology to another, for example, a computer connected via Ethernet, trying to query a device connected in a PAN (IEEE802.15.4). In addition, one of the requirements of this project is the aggregation of additional protection mechanisms for the transmission and this effect magnified the role of the gateway, which may works also as a transparent proxy.

The transparent proxy analyzes the data flow between client and server. This data stream can be modified e.g., by filtering, changing origin and destination, and may be blocked. In addition to modifications, the proxy provides extra features like exchanged-information storage, audititing through system logs,

traffic accounting, and SNMP MIB updating (Management Information Base) that will be used for remote management.

The management of proxy clients can be accomplished through two approaches: Web services and SNMP proxy agent. Web services allow retrieving information from devices that operate as services [9]. Services are routines that perform requests to the devices according to the technology supported by them (e.g., IEEE802.15.4, Bluetooth, Wi-Fi). These routines are accessed through remote requests. These requests are normally held on widespread protocols (e.g., HTTP, SOAP) [10]. Each of the protocols is associated with an approach to Web Services, such as Service Oriented Architecture (SOA) or Resource Oriented Architecture (ROA). The SNMP proxy agent is a conceptual database fulfilled by relevant information of management, i.e., one MIB [11]. The purpose of a MIB is to enable the management of devices that do not have SNMP agent installed. This management is accomplished through the proxy agent that accesses the managed devices using proprietary technologies. For example, a manager can send requests to an SNMP proxy agent, which retrieves the MIB site or collects the requested information directly from the device using the communication technology that has the same ability to use (Wi-Fi, Bluetooth).

The device used in the project is an access point that already has an SNMP agent. The SNMP agent is the necessary infrastructure for the SNMP proxy agent. With this existing infrastructure, the use of proxy agent solution becomes more interesting than build up a Web service. To meet the objectives of the project, the proxy agent requires modifications to allow recovery of information on each of the connected devices. This new information includes: (i) the type of device found, (ii) the unique identifier of the device, (iii) the energy level from the battery, (iv) a number on the measurement performed by the device, (v) time of the last request, (vi) the total time of operation of the device, (vii) the number of managed devices. Figure 2 shows the structure of the modules involved in communicating with IoT devices. The received data from the IoT devices are initially treated by the transparent proxy for changing the destination IP address (pre-configured by the manufacturer on some devices). Additionally, the communication is encrypted and data generated by the devices is extracted and update to the MIB (counters, status).

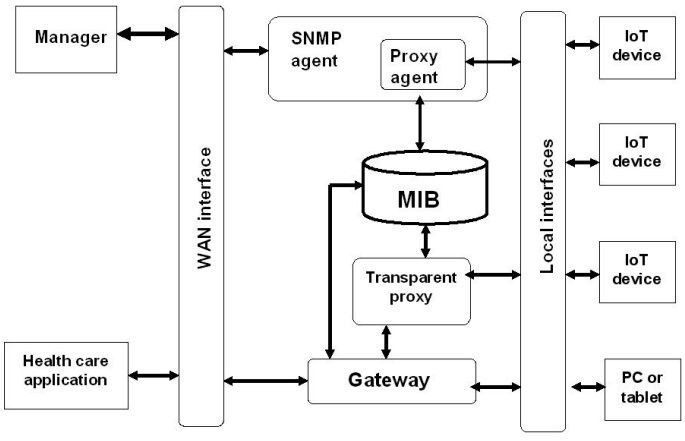

Figure 2. Infrastructure for IoT access via proxy agent

Figure 2 also shows the management requests for the IoT devices being manipulated by an SNMP Proxy Agent. When the manager sends commands to the agent, trying to get information about status or behavioral aspects of a device, the Proxy Agent will use any possible means to provide the information. Sometimes, this course of action could lead to implement translators to proprietary protocols or even store data from any previous communication that this device has done using the network and consequently, always keeping the MIB updated. This way, the information is forwarded back to the manager as an SNMP response message.

Any simple SNMP request must contain a unique identifier targeting managed objects. This unique identifier must be generated/configured during the activation process of the device. The activation process establishes an association with the device and the patient. This association is generated by combining a unique device identifier and the base unique identifier. Each patient uses his/her monitoring devices connected to a specific access point. This combination is registered in the telemonitoring system. Every time a new device is added, the external system records the access point used and stores the complete information in the MIB. Using this architecture it is possible to access and manage this kind of information just by using standards SNMP access. Managed objects hold the full data obtained from any device.

The transparent proxy is also the component responsible for identifying the originator device of the data, time stamping it, and applying encryption mechanisms to protect the transmission against unauthorized access.

Furthermore, considering that health workers should be allowed to access data of visited patients but only under policies regarding access and use of health data, an authentication system based was defined on a set of parameters including user id, password identification, time, device identification and geographic location of the device. This authentication system is used also to control access to patient own data. End-user devices like tablets and smartphones with GPS are being used for this extended security mechanism. An health worker should be able to access data from a patient using his/her mobile device while in the patient's home on a scheduled visit. But access is not permitted from other places or during periods of inactivity specifically linked to the patient in order to protect patient privacy and considering ethics considerations as discussed in [4]. These strategies aim to answer to security requirements of data authentication, access control, and client privacy. The requirement of resilience to attacks may be handled with more than one WAN connection using different kinds of communication like cell phones, cable modem, or even dial up and the switching from one to another may be managed by the gateway component. But this approach is still being incorporated to the solution because of operational characteristics of the access point selected to be used as infrastructure for this project, which intended to provide home healthcare services using devices already available on the market in contrast with other proposals using phone calls or implantable devices as described in [12].

The healthcare application runs in a remote server and manages telemonitoring applying filters on the data to prevent

reception of data from some health monitoring device that may be still active out of the follow-up period. Devices that were transferred from a home to another place without proper registration may send data to the system but this data should not be considered if they are no longer associated with a patient under monitoring. Many devices that comprise the landscape of Internet of Things do not have an unique identification and validation of data coming from these devices must be made by applying appropriate rules specific to each context.

VI. CONCLUSIONS

The experiment reported on using off-the-shelf IoT devices for an application of health telemonitoring at home showed that although feasible, the emergent market still does not offer flexible products that may be easily adapted for use in contexts other than the offered by the manufacturer and that allows only access to pre-configured servers in some cases. This points out the fact that IoT interoperability issues are still incipient despite not being considered a problem to develop a data transfer system connecting health care providers with patients [13] and the use of closed solutions may become a limitation when it comes to integrating IoT devices in a broader context. Some middleware proposals use Service-Oriented Architectures (SOA) mechanisms as basis for a middleware architecture in embedded networks [14] but in any case there is a need for standards to improve interoperability of devices especially in the case of healthcare devices. Needed standards should encompass open APIs, choice of interconnection interfaces, and configuration options of the operating mode of the monitoring/control device, including the aggregation of additional security mechanisms.

The embedded middleware proposed in this work offers a solution for interoperability enhancement and security management in a context using a special type of Internet of Thing devices for health monitoring with Wi-Fi interfaces. These kinds of devices cannot be connected directly to Internet for interoperability and security reasons, as it was discussed in this study. With the middleware it will be possible to provide an enhanced AAA (Authentication, Authorization and Accounting) service that it is especially important in this context as upheld in [4]. In this case, it was considered easier to create the middleware to manage and intermediate the communication between the “things” than to search for a solution that would modify the “things” due to the availability of the access point supporting the middleware software. Since the software used is free, this solution may be released as a product at no extra cost.

ACKNOWLEDGEMENTS

We thank RNP (Rede Nacional de Ensino e Pesquisa) and CTIC (Centro de Pesquisa e Desenvolvimento de Tecnologias Digitais para Informação e Comunicação) for financial support on the REMOA project.

REFERENCES

[1] G. Paré, K. Moqadem, G. Pineau, C. St-Hilaire, “Clinical effects of home telemonitoring in the context of diabetes, asthma, heart failure and hypertension: a systematic review,” J Med Internet Research, June 2010. Available at: http://www.jmir.org/2010/2/e21/ doi: 10.2196/jmir.1357

[2] L. Bos, A, Marsh, D. Carroll, S. Gupta, M. Rees, “Patient 2.0 empowerment,” International Conference on Semantic Web and Web Services, pp. 164–167, 2008.

[3] S. Babar, P. Mahalle, A. Stango, N. Prasad, R. Prasad, “Proposed security model and threat taxonomy for the Internet of Things (IoT),” Communications in Computer and Information Science, 89 CCIS, pp. 420-429, 2010.

[4] R.H. Weber, “Internet of Things - New security and privacy challenges,” Computer Law and Security Report, 26 (1), pp. 23-30, 2010.

[5] M. Sedlmayr, H. Prokosch, U. Münch, “Towards smart environments using smart objects,” Paper presented at. Studies in Health Technology and Informatics, vol. 169, pp. 315-319, 2011.

[6] Internet2, “Shibboleth.” Available at: http://shibboleth.internet2.edu/

[7] S. Katzenbeisse, M. Petković, “Privacy-preserving recommendation systems for consumer healthcare services,” Paper presented at the ARES 08 - 3rd International Conference on Availability, Security and Reliability, Proceedings, pp. 889-895, 2008.

[8] G. Delac, M. Silic, J. Krolo, “Emerging security threats for mobile platforms,” MIPRO, 2011 Proceedings of the 34th International Convention, pp.1468-1473, May 2011.

[9] T. Riedel, N. Fantana, A. Genaid, D. Yordanov. H.R. Schmidtke, M. Beigl, “Using web service gateways and code generation for sustainable IoT system development,” Internet of Things (IOT), pp.1-8, November-December 2010.

[10] N. Lim; S. Majumdar, B. Nandy, “Providing interoperability for resource access using web services,” Communication Networks and Services Research Conference (CNSR), 2010 Eighth Annual, pp. 236-243, 2010.

[11] S.S., Chavan, R. Madanagopal, “Generic SNMP proxy agent framework for management of heterogeneous network elements,” In Proceedings of the First international conference on Communication Systems and Networks (COMSNETS'09), pp. 1-6, 2009.

[12] Anh L. Bui, Gregg C. Fonarow, “Home Monitoring for Heart Failure Management”, Journal of the American College of Cardiology, vol. 59, Issue 2, 10 January 2012.

[13] Ladyzynski, P., Wojcicki, J.M., Foltynski, P. “Effectiveness of the telecare systems”. In IFMBE Proceedings, 37, pp. 937-940, 2011.

[14] Jesús Salceda, Iván Díaz, Juan Touriño, Ramón Doallo, “A middleware architecture for distributed systems management”, Journal of Parallel and Distributed Computing, vol. 64, Issue 6, pp. 759-766, June 2004.