GUIDELINES FOR DEVELOPING AN IOT-ENABLED APPLICATION FOR ENHANCED HOSPITAL MANAGEMENT

Teodor-Iulian VOICILA[1], Ana-George BOGDAN[2], Bogdan-Adrian ENACHE[3]
[1]National University of Science and Technology Politehnica Bucharest, Romania
[2]Business Consulting House SRL, Romania
[3]National University of Science and Technology Politehnica Bucharest, Romania
[1]iulian.voicila@upb.ro, [3]bogdan.enache2207@upb.ro

Keywords: IoT; Hospital; Management; Medical application.

Abstract: *The project "IoT Medical Asset Management Software (IMAMS)" aims to develop an innovative software application that responds to a critical component of the current activity of hospitals in Romania, respectively monitoring the state of operation of equipment and critical infrastructure in hospitals, compliance with maintenance plans, training to the people who will use the equipment and providing an overview of the availability of the equipment, regardless of the location where they are, by incorporating IoT solutions. The study presents the functional and non-functional requirements for the realization of an IoT medical application, along with an analysis between the differences in implementing the application using custom build or pre-build solutions.*

1. INTRODUCTION

The Internet of Things (IoT) has become an increasingly present technology in our daily lives, having a major impact on how we interact with the digital world. In recent years, IoT has evolved rapidly and started expanding into other areas such as industry, agriculture, healthcare and more [1], [2]. The Internet of Things refers to the network of devices made up of sensors that measure parameters in the environment, actuators that send feedback, processors that manage and store the generated data and nodes that coordinate the administration of these connected elements [3], [4]. For the efficient processing of the information generated by the IoT infrastructures, in order to capitalize on them in the decisions adopted at the level of the beneficiary communities, the use of specific Big Data and Big Data Analytics solutions is essential. Data acquisition and analysis, large-scale data analysis and storage, and data security are all topics covered by these solutions, BD and BDA [1].

In healthcare, IoT has started to be used to monitor patients in real time, improve the efficiency of the medical system and reduce costs [1], [3], [5]. For example, patient monitoring devices allow doctors to monitor patients' vital parameters in real time, such as blood pressure, pulse and temperature, and receive alerts when these values are outside the normal range, Fig 1 [6]–[8]. Moreover, IoT devices can be used to manage and monitor medical equipment in hospitals. By monitoring and recording data about he operation and condition of medical equipment, hospitals can reduce costs by planning ahead for maintenance and repair, and improve efficiency by eliminating downtime and increasing equipment availability [2], [9].

In terms of asset management applications that run or can run in hospitals, they are designed to collect data from IoT devices and to manage and monitor the health of devices, as well as to ensure that devices are updated, repaired, and replaced in a timely manner [10]. In addition, asset management solutions enable the detection and reporting of problems, thus enabling medical personnel to take immediate action to remedy any malfunction [11]. These systems are specifically developed for use in the hospital environment and must meet certain technical and security requirements [12], [13]. However, there

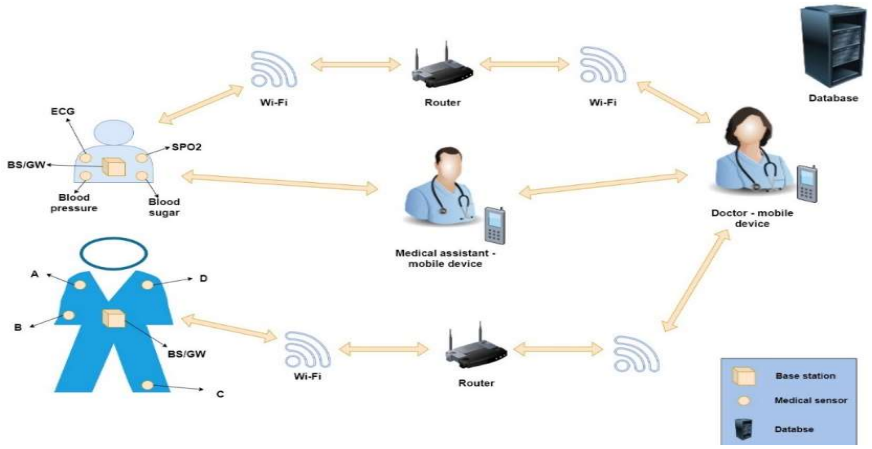

Fig. 1 Asset management application in hospitals

are still some issues that need to be addressed regarding the use of IoT in healthcare. One of these is related to data security as IoT devices collect and transmit a large amount of sensitive information about patients and medical equipment [10], [14]–[16]. There are also concerns about the interoperability of IoT devices, as different devices and applications may use different protocols and data formats [17], [18]. This diversity can lead to compatibility issues and difficulties in integrating IoT devices with existing systems.

Within this research project, the aim is to create an innovative software application that responds to a critical component of the hospitals' current activity, namely monitoring the state of operation of the equipment and critical infrastructure in hospitals, compliance with maintenance plans, training the people who will use the equipment and offering an overview of equipment availability, regardless of the location where they are, by incorporating IoT solutions. The main contributions of the paper are:

- Defining of the functional and non-functional specifications of an IoT medical application (SECTION 2);
- Presentation of the general architecture for the software application (SECTION 3);
- Analysis of the advantages and disadvantages between custom build and open-source/proprietary software solutions (SECTION 4).

2. THE SPECIFICATIONS OF AN IOT MEDICAL APPLICATION

A hospital asset management system involves complex data flows that are continuously managed to ensure optimal workflow. In general, there are three main types of data flows in such a system: the data flow from IoT sensors and devices; the data flow from medical devices; and the data flow from medical personnel. Therefore, below are presented the functional and non-functional requirements that a medical application based on IoT must fulfill.

A. FUNCTIONAL SPECIFICATIONS

To ensure efficient management of the data flows, it is important that a hospital asset management system to be properly designed and to have an appropriate network architecture. Thus, the following requirements have to be sustained [5], [11], [19]–[22]:

- The data flow from sensors and devices must be continuously monitored to ensure that the information is real-time and accurate;
- The data flow from medical devices must be monitored to ensure proper functioning and to detect any problems in a timely manner;
- The data flow from medical staff must be monitored to ensure that equipment is being used appropriately and to identify any inconsistencies in the work process;
- Equipment that allows access to sensitive information must be protect by authentication (password, card or biometric);
- The data storage method must be taken into account, which can be local, server,

or cloud based, along with a back-up functionality;
- The redundancy of critical components, like the server or important medical devices, have to be considered.

B. NON-FUNCTIONAL SPECIFICATIONS

Smart solutions for hospitals must comply with several rules and regulations, including those regarding personal data protection, information security, patient safety and operational efficiency. The following non-functional specifications have to be considered for an IoT medical application [5], [11], [19]–[22]:

- Compliance with security and privacy standards (robust authentication and authorization, data encryption, access control, auditability, compliance with various regulations (ISO27001, HIPA, GPDR etc.);
- Connectivity: the solution must support standard communication protocols such as Bluetooth, Wi-Fi, ZigBee, Z-Wave or other wireless communication protocols so that it can communicate with IoT devices;
- Integration capability: the solution must have the ability to integrate with other systems and applications within the hospital, such as EMR (Electronic Medical Records) and HIS (Hospital Information System);
- Scalability: the solution must be scalable so that it can handle a large number of IoT devices and can be expanded over time as the hospital grows;
- User-friendly interface: the solution must provide an easy-to-use interface that allows hospital staff to monitor and manage IoT devices and associated data;
- Performance and availability: the solution must provide high performance and availability so that it can handle the large volume of data generated by IoT devices and operate continuously without interruption;
- Support and maintenance: the solution must provide support and maintenance to ensure the proper functioning of the system over time and to fix any problems that may arise.

IoT solutions that are considered to be drugs or that may compromise the safety and privacy of medical data are categorically prohibited. Thus, intelligent solutions that are compatible with the requirements mentioned above must be used.

3. THE GENERAL ARCHITECTURE OF AN IOT MEDICAL APPLICATION

The general scheme of a hospital asset management system, Fig 2, which includes the data collection process and its management, as well as the interaction with end users, has the following components.

Sensors and devices: these are the elements that collect data about assets. For example, sensors can collect information about temperature, humidity, pressure, vibration and other aspects related to the operation of assets;

Connectivity: data collected from sensors and devices is transferred to an asset management platform through various connectivity technologies such as Bluetooth, Wi-Fi, Zigbee or other specific protocols;

Asset management platform: this is the central part of the asset management system and is responsible for managing data collected from sensors and devices. This may include the software and hardware needed to process the data, as well as analysis and reporting tools. For example, the analysis and reporting sub-element is responsible for analyzing data collected from assets and generating relevant reports. This may include data analysis tools, such as artificial intelligence algorithms or machine learning as well as reporting tools, such as graphs, tables or text reports. The data integration sub-element is responsible for collecting and generating data in various formats (CSV, XML) compatible with the protocol through which the messages are transferred via sensors, medical devices and so on. After that, the data analysis sub-element analyze and verify the access permission, the generation of alerts, the level of the authentication factor, the state of the devices, and allow data to be sent to the data transfer sub-element to share the information through appropriate way (Bluetooth, Wi-Fi). Data Storage & Management sub-element saves the information received from sensors, medical devices and other sub-elements in a

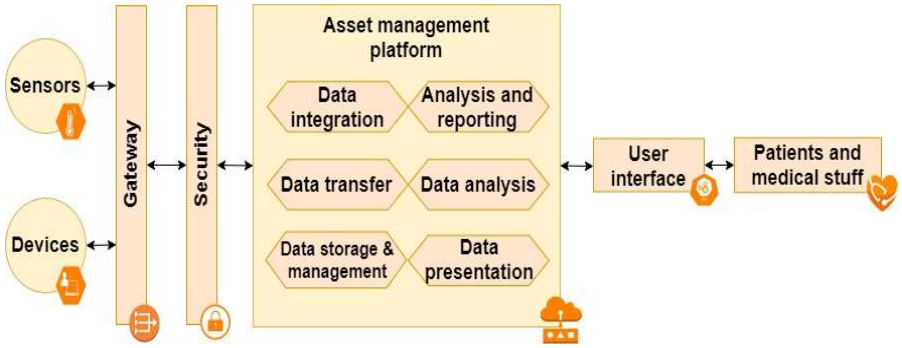

Fig. 2. General architecture of an IoT medical application

database provided with several levels of security depending on the sensitivity of the data. Finally, the data presentation sub-element implements the necessary interface for the operability of the information with users (user login interface, user monitoring interface.

Security: this is the protection component which verify the integrity of the data, allows authentication based on user access, sends malfunction notification etc.

User interface: this is the interface through which end users, like patients and medical staff, can interact with the asset management system. This can include a variety of interfaces such as mobile applications, web platforms or special devices such as display panels.

Each sub-element of the asset management platform is also called a microservice (authentication service, data storage service, data analysis service, alert service etc.). These microservices are an architectural approach to software development where the application is broken down into smaller, independent components called microservices. These are standalone components that can be deployed, updated, and scaled separately from the other application components [13], [23]. One of the advantages of using microservices is that they can be used to enable easy integration of IoT devices into an existing hospital asset management system without the need to make significant changes to the application. This reduces development and implementation time and costs.

4. SOFTWARE SOLUTIONS USED

The IMAMS research project aims to create a software application that allows monitoring the operating status of the equipment and providing an overview of the availability of the medical equipment, by incorporating IoT solutions. The application will work on the same equipment as the existing HIS in hospitals. The hardware load is given strictly by the introduction of IoT equipment in the client's configuration. Due to their small size and ease of use, they will not be noticed as an additional logistical burden, so the hardware impact is minimal. Users will have a Web interface at their disposal and will not require components dedicated to the stations, neither hardware nor software. Security will be provided by user/password, similar or even the same as HIS. IoT Assets Management application has the effect of ensuring continuity in the operation of medical equipment, by following the maintenance plan, and represents the first application of this kind to be implemented in Romania. However, the problem encountered in this stage of the project is whether it is feasible and worth building the application from scratch or purchasing an open-source/proprietary software modules that meet the application's requirements.

Table 1. Characteristics comparison of custom-build and pre-build applications

Characteristic	***Custom-build***	***Pre-build***
Scalability	*High*	*Medium*
Flexibility	*High*	*Medium*
Customize	*High*	*Medium*
Capability	*High*	*High*
Cost	*High*	*Medium*
Implementation time	*High*	*Low*
Security	*Depends*	*High*
Interoperability	*Medium*	*Medium*

Considering the possibility of expanding the application and even implementing it in other hospitals with other requirements, then scalability plays an important role. A pre-build application has its limitations, which are mostly related to the collaborating company and their expansion capacity. Instead, a custom-build application can be endlessly improved as technological advances or new requirements arise due to changing hospital infrastructure. In other words, as the project grows and changes, flexibility and customization come hand in hand for a custom-build application that are less possible with a pre-build. IoT technology is widely used and developed by many companies at the moment, therefore the capability of pre-build applications is as high as the custom one. However, the cost is obviously much more than a preconfigured solution [24]. Also, the implementation time of an application created from scratch is much longer compared to solutions already on the market. While security is guaranteed for pre-existing solutions, it depends on the time and budget spent on its implementation for unique approaches. Interoperability in the case of IoT systems is ensured by the contracting company, most of the time for its own products and partially on external ones, while custom-build applications achieve it through the design and analysis of the infrastructure. It is clear that each approach has its benefits and drawbacks, as can be seen in Table I, and the right solution depends on the application requirements. In this case, the circumstances require the application to comply with Romanian legislation, in addition to other specific demands that require dedicated solutions. Therefore, it is worth the effort and time needed to create such an application to achieve certain specifications and align with the country's regulations.

5. CONCLUSIONS

Regarding the minimum technical specifications for IoT devices used in hospitals, they should comply with specific technical and safety regulations, as well as comply security and privacy standards to protect patient data and other sensitive information. They should also be interoperable with other systems and medical devices and provide a user-friendly and easy-to-use interface. The study shows that the realization of an IoT medical application is a serious project in which the requirements must be defined very carefully, and that requires the implementation of a customized solution that allows legal compliance and further development. To successfully use IoT devices within an asset management system, it is important to have a solid IT infrastructure and a well-developed communications network. It is also important to have a well-defined strategy for deploying IoT devices and be prepared to adapt to changes while aligning with legal and regulatory requirements. Overall, integrating IoT equipment into an existing asset management system can provide multiple benefits in terms of tracking and monitoring medical equipment, thereby improving the efficiency and quality of medical services.

ACKNOWLEDGMENT

The project IoT MEDICAL ASSET MANAGEMENT SOFTWARE (IMAMS) is financed by the Competitiveness Operational Program 2014-202, co-financed by the European Regional Development Fund, call code: POC/524/2/2/Supporting the increase of added value generated by the ICT sector and innovation in the field through the development of clusters, Action 2.2.1 call 2, Information and Communication Technology (ICT) priority axis for a competitive digital economy.

REFERENCES

[1] T. Saheb and L. Izadi, "Paradigm of IoT big data analytics in the healthcare industry: A review of scientific literature and mapping of research trends," *Telemat. Inform.*, vol. 41, pp. 70–85, Aug. 2019, doi: 10.1016/j.tele.2019.03.005.

[2] S. Lim and R. Rahmani, "Toward Semantic IoT Load Inference Attention Management for Facilitating Healthcare and Public Health Collaboration: A Survey," *Procedia Comput. Sci.*, vol. 177, pp. 371–378, 2020, doi: 10.1016/j.procs.2020.10.050.

[3] A. Rejeb *et al.*, "The Internet of Things (IoT) in healthcare: Taking stock and moving forward," *Internet Things*, vol. 22, p. 100721, Jul. 2023, doi: 10.1016/j.iot.2023.100721.

[4] F.-C. Adochiei *et al.*, "Electronic System for Real-Time Indoor Air Quality Monitoring," in *2020 International Conference on e-Health and Bioengineering (EHB)*, Iasi, Romania: IEEE, Oct. 2020, pp. 1–4. doi: 10.1109/EHB50910.2020.9280192.

[5] R. Zgheib, G. Chahbandarian, F. Kamalov, H. E. Messiry, and A. Al-Gindy, "Towards an ML-based semantic IoT for pandemic management: A survey of enabling technologies for COVID-19," *Neurocomputing*, vol. 528, pp. 160–177, Apr. 2023, doi: 10.1016/j.neucom.2023.01.007.

[6] F.-C. Adochiei *et al.*, "Brain Mapping using a Blockchain Approach," in *2019 E-Health and Bioengineering Conference (EHB)*, Iasi, Romania: IEEE, Nov. 2019, pp. 1–4. doi: 10.1109/EHB47216.2019.8970089.

[7] F. C. Argatu, F. Constantin Adochiei, I. R. Adochiei, R. Ciucu, V. Vasiliki, and G. Seritan, "A Scalable Real-Time Biomonitoring Platform," in *2019 E-Health and Bioengineering Conference (EHB)*, Iasi, Romania: IEEE, Nov. 2019, pp. 1–4. doi: 10.1109/EHB47216.2019.8970064.

[8] M. Oproescu, V. G. Iana, N. Bizon, D.-C. Anghel, A. Sirghie, and O. C. Novac, "Mechanical ventilation device with adapted parameters to assist patients infected with the SARS-CoV-2 virus," in *2020 12th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, Bucharest, Romania: IEEE, Jun. 2020, pp. 1–6. doi: 10.1109/ECAI50035.2020.9223128.

[9] A. Belfiore, C. Cuccurullo, and M. Aria, "IoT in healthcare: A scientometric analysis," *Technol. Forecast. Soc. Change*, vol. 184, p. 122001, Nov. 2022, doi: 10.1016/j.techfore.2022.122001.

[10] P. Hegde and P. K. R. Maddikunta, "Amalgamation of Blockchain with resource-constrained IoT devices for healthcare applications – State of art, challenges and future directions," *Int. J. Cogn. Comput. Eng.*, vol. 4, pp. 220–239, Jun. 2023, doi: 10.1016/j.ijcce.2023.06.002.

[11] M. Haghi Kashani, M. Madanipour, M. Nikravan, P. Asghari, and E. Mahdipour, "A systematic review of IoT in healthcare: Applications, techniques, and trends," *J. Netw. Comput. Appl.*, vol. 192, p. 103164, Oct. 2021, doi: 10.1016/j.jnca.2021.103164.

[12] P. Kumar, S. K. Sharma, and V. Dutot, "Artificial intelligence (AI)-enabled CRM capability in healthcare: The impact on service innovation," *Int. J. Inf. Manag.*, vol. 69, p. 102598, Apr. 2023, doi: 10.1016/j.ijinfomgt.2022.102598.

[13] H. Siddiqui, F. Khendek, and M. Toeroe, "Microservices based architectures for IoT systems - State-of-the-art review," *Internet Things*, vol. 23, p. 100854, Oct. 2023, doi: 10.1016/j.iot.2023.100854.

[14] F. Ullah, C.-M. Pun, O. Kaiwartya, A. S. Sadiq, J. Lloret, and M. Ali, "HIDE-Healthcare IoT Data Trust ManagEment: Attribute centric intelligent privacy approach," *Future Gener. Comput. Syst.*, vol. 148, pp. 326–341, Nov. 2023, doi: 10.1016/j.future.2023.05.008.

[15] O. O. Okediran, "A METHODICAL REVIEW OF SECURITY AND PRIVACY ISSUES IN CLOUD-BASED ELECTRONIC HEALTH RECORDS", *University of Pitesti Scientific Bulleting Series ECS, 20(1), 1-12*.

[16] O. O. Okediran, "A SECURITY SCHEME FOR PATIENT INFORMATION PRIVACY IN DIGITAL MEDICAL IMAGING", *University of Pitesti Scientific Bulleting Series ECS, 19(2), 13-24*.

[17] H. Zakaria, N. A. Abu Bakar, N. H. Hassan, and S. Yaacob, "IoT Security Risk Management Model for Secured Practice in Healthcare Environment," *Procedia Comput. Sci.*, vol. 161, pp. 1241–1248, 2019, doi: 10.1016/j.procs.2019.11.238.

[18] Md. O. Qays, I. Ahmad, A. Abu-Siada, Md. L. Hossain, and F. Yasmin, "Key communication technologies, applications, protocols and future guides for IoT-assisted smart grid systems: A review," *Energy Rep.*, vol. 9, pp. 2440–2452, Dec. 2023, doi: 10.1016/j.egyr.2023.01.085.

[19] M. Dadhich, S. Poddar, and K. K. Hiran, "Antecedents and consequences of patients' adoption of the IoT 4.0 for e-health management system: A novel PLS-SEM approach," *Smart Health*, vol. 25, p. 100300, Sep. 2022, doi: 10.1016/j.smhl.2022.100300.

[20] S. Kim and S. Kim, "User preference for an IoT healthcare application for lifestyle disease management," *Telecommun. Policy*, vol. 42, no. 4, pp. 304–314, May 2018, doi: 10.1016/j.telpol.2017.03.006.

[21] F. Kammuller, J. C. Augusto, and S. Jones, "Security and privacy requirements engineering for human centric IoT systems using eFRIEND and Isabelle," in *2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA)*, London, United Kingdom: IEEE, Jun. 2017, pp. 401–406. doi: 10.1109/SERA.2017.7965758.

[22] G. C. Seritan *et al.*, "Guidelines for Small Size Samples Biostatistics in Current Medical Practice," in *2019 E-Health and Bioengineering Conference (EHB)*, Iasi, Romania: IEEE, Nov. 2019, pp. 1–4. doi: 10.1109/EHB47216.2019.8970086.

[23] S. B. Atitallah, M. Driss, and H. B. Ghzela, "Microservices for Data Analytics in IoT Applications: Current Solutions, Open Challenges, and Future Research Directions," *Procedia Comput. Sci.*, vol. 207, pp. 3938–3947, 2022, doi: 10.1016/j.procs.2022.09.456.

[24] I. V. Evdokimov, A. R. Jihad Alalwan, R. Y. Tsarev, T. N. Yamskikh, O. A. Tsareva, and A. N. Pupkov, "A cost estimation approach for IoT projects," *J. Phys. Conf. Ser.*, vol. 1176, p. 042083, Mar. 2019, doi: 10.1088/1742-6596/1176/4/042083.