The 8th IEEE International Conference on E-Health and Bioengineering - EHB 2020
Grigore T. Popa University of Medicine and Pharmacy, Web Conference, Romania, October 29-30, 2020

Security and Privacy Risks for Remote Healthcare Monitoring Systems

Marilena Ianculescu[1,2], Dora Coardoș[1], Ovidiu Bica[1], Victor Vevera[1]
[1]National Institute for Research and Development in Informatics, Bucharest, Romania
[2]University Politehnica of Bucharest, Computer Science Department, Bucharest, Romania
e-mail: {marilena.ianculescu, dora.coardos, ovidiu.bica, victor.vevera}@ici.ro

***Abstract*— Remote healthcare monitoring systems have increasingly become a reliable solution for delivering personalized, less intrusive and patient-friendly healthcare services. Internet of Things technology is an important driver for sustaining a large range of the capabilities of these systems, including the access to a huge amount of various health data. As this data are considered highly sensitive due to the personal feature, security and privacy threats and attacks are very likely to target the vulnerabilities of the IoT devices, network connectivity, data storage etc. This presents a brief overview of the vulnerabilities of the above-mentioned systems and a proposed solution for addressing them from the designing stage. For this purpose, a synthesis of security and privacy vulnerabilities, basic requirements and countermeasures associated distinctively with each level of the IoT-based architecture of RO-SmartAgeing system is put forward.**

Keywords*— *remote healthcare monitoring systems, security and privacy requirements, vulnerabilities, countermeasures.

I. Introduction

The late broad spreading of the use of Internet of Things (IoT) technology has imposed as a natural direction its extensive usage in the healthcare domain; among its capabilities, IoT facilitates a reliable link between a patient and healthcare units [1]. Internet of Things (IoT) represents one of the most explosive growths in nowadays technology; it is estimated that 41.6B IoT will be connected by 2025 and will generate 79.4 zettabytes of data [2]. Meanwhile, the vulnerability of IoT devices is augmented by a low rate (around 25%) of encryption for IoT devices, platforms and data repositories according to [3]. Another recent study [4] underlined that 42% of IoT devices will count fundamentally on digital certificates for identification and authentication by 2022. More important, all collected data are used in different businesses where people health is important and sensitive.

A remote healthcare monitoring system (RHMS) comprises (smart) devices, IoT and wireless sensor networks for gathering, storing and real-time analyzing of various medical parameters [5]. Due to the diversity of IoT technology, associated communication networks and the strong sensitive feature of heath data, significant issues related to security and privacy have to be attentively taken into consideration. Effective and flexible security protocols and mechanisms are needed to prevent, identify and block any virulent interference with the RHMS [6]. Thus, a reliable framework has to be designed for ensuring the confidentiality, authentication, authorization and availability of the system.

This paper highlights the most important issues that have to be taken into consideration for addressing the security and privacy risks for RHMS. The paper is written around different Sections. Section II states some basic elements regarding the vulnerabilities of RHMS in relation with security and privacy risks. Section III presents an example of how the malicious attacks can be addressed in the designing stage of a RHMS. RO-SmartAgeing system is introduced as a case study, its conceptual architectural requirements and issues regarding security and privacy risks are described and discussed. Section IV sums up the above points.

II. Vulnerabilities of Remote Healthcare Monitoring Systems in Terms of Security and Privacy

In cybersecurity, vulnerability is perceived as a deficiency or failure in the code of a system or device that can be worked off through a cyber-attack to obtain unauthorized access or to execute malicious operations. Vulnerabilities provide breaches to alter the code and data, to ingress into data storage, to install malware. These attacks address the confidentiality, integrity, or availability (the so-called "CIA triad") of the resources of the system [7]. IoT-based devices provide and deliver an increasing and comprehensive amount of a great diversity of data, which are particular sensitive in healthcare domain. Colligating this data with all the other one and information regarding a patient or a medical entity implies the existence of a valuable target for cyber-attackers. Therefore, the security and privacy risks are encountered since the data gathering till its storage into the cloud.

A. Security and privacy vulnerabilities

These vulnerabilities can be classified into several types, based on different criteria - such as the presence of the vulnerability, its causes or usages. The main categories within a

IEEE 978-1-7281-8803-4/20/$31.00 ©2020 IEEE

monitoring system comprise vulnerabilities at different levels [8]:

- at *the physical level*: they are related with a straightforward ingression to the devices/technology that can be accessed, controlled or physically damaged; examples of specific attacks are: Node Tampering, RF Interference on RFIDs, Malicious Node Injection, Malicious Code Injection [9];

- at *the software level:* they are associated with the malfunction of the software due to hidden flaws; examples of specific attacks are: Malicious Scripts, Denial-of-Service (DoS), Phishing Attacks, Virus, Worms and Spyware;

- at *the network level*: they are linked with the network insecurity due, for instance, to the use of low-cost devices and software services that rely heavily on wireless networks such as Wi-Fi (which are known to be quite vulnerable to various intrusions); examples of specific attacks are: Traffic Analysis attacks, RFID Spoofing, RFID Cloning, RFID Unauthorized Access, Routing Information attacks, Unauthorized Router Access, Man-in-the-Middle (MITM) attacks, DoS, Brute-force attacks, and Traffic Injections;

- at *the encryption level:* they are correlated with the violation of the encryption structure used in systems like those that are based on IoT; examples of specific attacks are: Side Channel Attacks, Cryptanalysis Attacks, or MITM Attack;

- at *the human level:* they are related with the end-user errors which can provide unauthorized access to databases and system code (commonly because of the lack of specific process controls and the use of weak passwords); examples of specific attacks are: Email Phishing or Ransomware Viruses.

B. Security and privacy requirements

In a RHMS, aspects addressing security and privacy issues must be carefully considered in a direct compliance with legal and ethical rules on confidentiality, such as the EU General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) in USA, where it's stated that only authorized persons can access these data [10].

The main data security and privacy requirements in the design and implementation of a RHMS [6] are presented as follows:

- For the data:

- *The confidentiality* of patient data means that the gathered, sent and stored medical information can only be accessed by authorized persons [11]. Data confidentiality is usually obtained by encryption/decryption;

- *Data access control* defines a privacy policy and prevents unauthorized access to patient information. Data access roles must be set up through associated different access rights;

- *Data availability* allows the patient data to always be available to the physician/patient/healthcare provider;

- *Non-repudiation* ensures the integrity and authenticity of data. A common way to ensure non-repudiation is to use digital signatures during communication.

- For the data communication:

- *Data integrity* implies data accuracy (correctness and consistency) throughout the whole transmission process, ensuring that no changes have been made to data before reaching storage.

  The integrity of data in healthcare is decisive because data reflects diagnoses, treatments, or health status of the pacient [12]. One mechanism for achieving data integrity is the use of a message authentication code used both by the sender and the receiver to check if data is not maliciously altered;

- *Data authentication* must ensure that the data is sent by a trusted sender. A message authentication code with a shared secret key can be used. If such a mechanism is missing, it might happen that a fake sender, who appears to be legitimate, sends false data for storage or gives incorrect treatment instructions to a patient or has access to personal information.

  The digital signature is one of the most trustful processes for ensuring authenticity in this case.

- For the data storage:

- *Reliability,* one of the most critical properties when it comes to data storage, ensures fast retrieval of patient data;

- *Storage space:* remote monitoring during a pandemic period may results in huge amount of data that need specific volumes and add new security issues (like consistency in distributed data storage).

III. Managing the Security and Privacy Risks in a RHMS

A. Short presentation of RO-SmartAgeing system

"*Non-invasive monitoring and health assessment of the elderly in a smart environment (RO-SmartAgeing)*" is a research project coordinated by ICI Bucharest that is in-progress in its fourth phase, i.e. the detailed design. The developed system aims to provide a practical alternative to the clinical and social services through a comprehensive management of an elderly person's related data that is collected in a non-clinical smart environment and through the setting up of extensive capabilities for assistance and support of medical decisions. The personalized smart environment comprises diverse IoT, smart sensors and devices for collecting health, ambient, motion and lifestyle parameters [13], [14].

B. Basic requirements for RO-SmartAgeing system security architecture

RO-SmartAgeing system is based on a hybrid architecture, which combines the multilevel IoT architecture with the microservices-based one, in order to collect, store and process complete, reliable, relevant, current data gathered in a smart environment. Due to the highly sensitive feature of the health data, a special attention is paid to the security and privacy characteristics of the system.

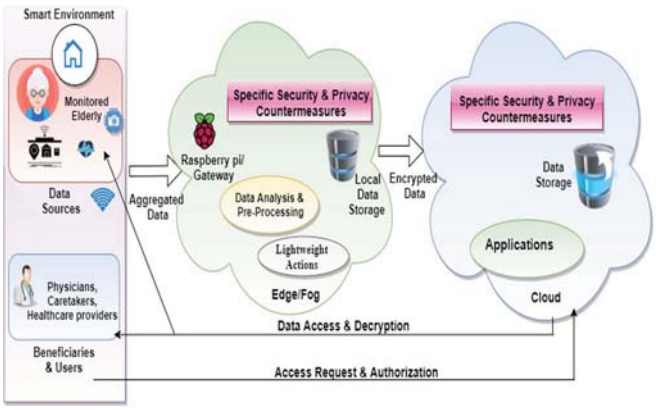

Fig 1. Conceptual architecture requirements for security and privacy concerns.

As it is presented in Fig. 1, the concerns about these characteristics are tackled distinctively at each level of the architecture, due to the fact that the cyber-attacks might be specific.

For instance, at the Edge/Fog Layer, examples of particular attacks categories are data tampering, DoS, malware protection, wireless security or virtualization issues [15]. At the Cloud level, among the specific attacks that can be mentioned are DoS, Distributed Denial of Service (DDoS) [16], code injection to access users' data, phishing, MITM attack.

In Table 1, for each level of RO-SmartAgeing architecture are summarized the main vulnerabilities, the basic security and privacy requirements and specific countermeasures.

TABLE I. ADDRESSING SECURITY AND PRIVACY ISSUES IN RO-SMARTAGEING SYSTEM

RO-SmartAgeing Layers	Main vulnerabilities	Basic security and privacy requirements	Countermeasures
Visualisation/ Action Layer	– Unauthorized access – Data breach	– Availability – Authorization – Integrity – Confidentiality	– End user AAA controls (authentication, authorization, accounting) – Secure communication protocols – Data masking – Decoy technique for user behavior profiler
Cloud Layer	– Identity authentication – Database Security – Compromised data via malicious software – Data recovery – Unauthorized data, activity and Virtual Machine monitoring	– Authentication – Policy-based access control – Intrusion detection – Identification of malicious data – Key management – Encryption storage – Integrity – Confidentiality – Multiplied backup databases – Data leakage prevention	– Selective Access control (as Attribute-Based Encryption) – Cryptographic protocols for data at Cloud – Database-level encryption (as Transparent Data Encryption) – Encryption protocol standards (like Secure Sockets Layer (SSL) and Internet Protocol Security (IPSec) – Privacy-preserving protocols – Specific Cloud computing platform security – Virtual machine software – Pseudonymization – Key management protocols (as IEEE 802.15.4)
Fog/Edge Layer	– Unauthorized access – Data breach – Different service providers due to distinct deployment needs	– Device and User Authentication – Intrusion detection – Identification of malicious data – Encryption storage – Confidentiality – Integrity – Key management – Data leakage prevention	– Authentication schemes – Intrusion detection methods – Cryptographic protocols for data at Edge/Fog (as Transport Layer Security- TLS) – Record-level encryption (using AES or Rivest–Shamir–Adleman -RSA) – Privacy-preserving protocols – Key management protocols (as ISKAMP and IKE protocols) – Mechanisms to clearly identify the fog nodes among the others
Communication Layer	– Data breach (through attacks like Distributed denial-of-service attacks - DDoS- Denial of Service -DoS) – Compatibility issues – Heterogeneity of network components – Lack of appropriate protocols in wireless communications	– Authentication – Key agreement – Intrusion Detection – Confidentiality – Integrity – Non-repudiation	– Communication security protocols (as IEEE 802.15.4, IEEE 802.15.6, ZigBee, Wired Equivalent Privacy (WEP), Wi–Fi Protected Access (WPA), Bluetooth, 3G/4G/5G) – Key pre-distribution protocols (as Quantum Key Distribution) – Identity authentication – Encryption mechanisms (as Symmetric key encryption, Conventional Public Key Encryption Identity Based Encryption) – Firewalls – Challenge–response authentication (as Bluetooth link key) [17] – Public Key Exchange (PKE) – Secure Wi-Fi router (as Norton Core, F-Secure Sense)
Perception Layer	– Node authentication – Timing attacks – Fake nose attacks – Tampering the identity information of a device – Malicious devices providing false information – Ability to securely update the device	– Authentication – Confidentiality – Privacy – Integrity – Availability – Lightweight encryption – Key agreement – Localization – Self-healing	– Access control (as Role-Based Access Control – RBAC, Attribute Based Access Control -ABAC) – IoT security (like Cryptographic algorithms as Secure Hash Algorithm -SHA- and Advanced Encryption Standard -AES [18], Routing protocols security, Public Key Infrastructures – PKI, etc.) – RFID security (as Protocol security, Base station security, Tag encode security, etc.) – Device tampering detection (with tamper detection sensors) – Intrusion detection methods – Self-healing methods – Secure update mechanisms

C. Discussion

The core of RO-SmartAgeing system is based on healthcare data; therefore, taking into consideration the sensitive feature of it, implementing proper data encryption countermeasures has a crucial importance. There are many aspects regarding security and privacy that must be addressed in a distinct way, depending on each of the five layers of the architecture and specific issues associated with technologies used inside RO-SmartAgeing system. Some of the envisioned ones are highlighted as follows:

For instance, among the cyber-attacks that are usually associated with the Visualisation/Action Layer are Malicious code injection, DoS, DDoS, or Phishing. The most appropriate countermeasures are *End user AAA control, Encryption mechanisms, Intrusion detection methods* or *Decoy techniques for user behavior profiler* that aim to identify the attacks and abnormalities. At the Cloud and Fog/Edge layers level, for attacks like Malicious Insider, Malware and DoS attacks, *Pseudonymization* is a proper countermeasure that implies that all personal identifying data is substituted with a pseudonym generated aleatory. *Record-level encryption* might be more appropriate for the sensitive healthcare data than the *database-level security*, usually ensured by the cloud providers, as every unique record is encrypted using its original key. At the Communication Layer level, where MITM, Spoofing Flooding, DoS and Storage attacks are among the most common ones in an IoT architecture, confidentiality can be strengthened by using *TLS*, a security protocol for communication in internet compatible with a consistent number of internet protocols [19], or *Message Authentication Code* and *Encryption mechanisms*. The elderly-related data in the smart environment that enframes the RO-Smart Ageing system is manipulated by various devices which functionalities are subject to some of the most common cyber-attacks. At the Perception layer level, for preventing specific attacks like Eavesdropping, Radio Interference, Node capture, DoS, Tampering, Jamming or Routing and Timing attacks, envisioned countermeasures are *Access Control and Device tampering detection or PKI* that is a flexible and scalable countermeasure able to ensure that the device has a unique and traceable identity or to protect the communication with it.

IV. Conclusions

IoT can be perceived both as a main driver for the more intensive nowadays implementation of RHMS, and a risk factor from the point of view of security and privacy concerns related to the health data. This paper aimed to emphasize the challenges that have to be addressed even from the designing phase of a RHMS in order to cope with potential vulnerabilities. RO-SmartAgeing system was presented as a study case for demonstrating how the security and privacy risks can be managed in a distinct way for each level of its IoT-based architecture. Some limitations of the proposed solution are clearly associated with the ongoing designing phase, but, as the system is developed, they will be worked out for addressing the current and future cyber-attacks.

ACKNOWLEDGMENT

The authors gratefully acknowledge the contribution of the Romanian Ministry of Research and Innovation with regard to the funding of the projects "*RO-SmartAgeing - Non-Invasive Monitoring System and Health Assessment of the Elderly in a Smart Environment*" for the period 2019-2022.

REFERENCES

[1] H. Kaur, M. Atif, R. Chauhan, "An Internet of Healthcare Things (IoHT)-Based Healthcare Monitoring System", Advances in Intelligent Computing and Communication, vol **109**, Springer, 2020, pp 475-482.

[2] C. MacGillivray, D, Reinsel, "Worldwide Global DataSphere IoT Device and Data Forecast" IDC Report, 2019, Doc # US45066919.

[3] nCipher, "2019 Global Encryption Trends Study", 2019, https://www.nciphersecurity.co.uk/2019/global-encryption-trends-study.

[4] Ponemon, "2019 Gobal PKI and IoT Trends Study", nCipher Security, 2019, https://go.ncipher.com/rs/104-QOX-775/images/2019-Ponemon-Global-PKI-and-IoT-Trends-Study-es.pdf?_ga=2.136729459.2134188774.1594305782-2128812512.1594305782.

[5] C. Z. Rădulescu, A. Alexandru, L. Băjenaru, "Health parameters correlation in an IoT monitoring, evaluation and analysis framework for elderly," Proc. 23rd International Conference on System Theory, Control and Computing, 10.1109/ICSTCC.2019.8886117, 2019, pp. 531-536.

[6] H. Fotouhi, A. Causevic, K. Lundqvist, M. Bjorkman, "Communication and Security in Health Monitoring Systems - A Review", Proc. 40th IEEE Computer Society International Conference on Computers, Software & Applications, 2016.

[7] K. Brauer, "Authentication and Security Aspects in an international multi-user network", Thesis (UAS), Information Technology European Computer Science, 2011.

[8] D. T., Handler, L., Hauge, A., Spognardi, N. Dragoni, "Security And Privacy Issues in Healthcare Monitoring Systems: A Case Study". Proc. 10th International Joint Conference on Biomedical Engineering Systems and Technologies, Vol. **5**, 2017, pp. 383-388.

[9] H. F. Atlam, G. B. Wills, "IoT Security, Privacy, Safety and Ethics", Digital Twin Technologies and Smart Cities, Springer, 2020.

[10] Y. Sun, F. P.-W. LO, .B. LO, "Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey", IEEE ACCESS, 2019.

[11] S. A. M. Muhammad, A. Muhammad, A. Tahir, K. Naila, N. S. Mehak, A. Muhammad, "Wireless Body Area Network Security and Privacy Issue in E-Healthcare", International Journal of Advanced Computer Science and Applications, Vol. 9, No. 4, 2018.

[12] F. Alsubaei, A. Abuhussein, S. Shiva, "Security and privacy in theInternet of medical things: Taxonomy and risk assessment", Proc. IEEE 42nd Conf. Local Comput. Netw. Workshops, 2017, pp. 112_120.

[13] M. Ianculescu, A. Alexandru, G. Neagu, F. Pop, "Microservice-Based Approach to Enforce an IoHT Oriented Architecture". In 2019 E-Health and Bioengineering Conference (EHB) 2019, pp. 1-4, IEEE.

[14] D.N. Nicolau, A. Alexandru, M. Ianculescu, "An IoT, Virtual Machines and Cloud Computing-based Framework for an Optimal Management of Healthcare Data Collected from a Smart Environment. A Case Study: RO-Smart Ageing Project", Informatica Economica. 2019 Jul 1;23(3).

[15] S. Khan, S. Parkinson, Y. Qin, "Fog computing security: a review of current applications and security solutions". Journal of Cloud Computing, 6. 19. 10.1186/s13677-017-0090-3, 2017.

[16] B.C. Chifor, I. Bica, V.V. Patriciu, F. Pop, "A security authorization scheme for smart home Internet of Things devices", Future Generation Computer Systems, 86, 10.1016/j.future.2017.05.048, 2018, pp. 740–749.

[17] J. Padgette, J. Bahr, M. Batra, M. Holtmann, R. Smithbey, L. Chen, K. Scarfone, "Guide to Bluetooth Security", NIST Special Publication 800–121 Revision 2, 2017.

[18] S. Zeadally, S., A. K Das., N. Sklavos, "Cryptographic technologies and protocol standards for Internet of Things" Internet of Things", Internet of Things, Elsevier, 2019, https://doi:10.1016/j.iot.2019.100075.

[19] G. Nebbione, M.C. Calzarossa, "Security of IoT Application Layer Protocols: Challenges and Findings". Future Internet. 12. 55. 10.3390/fi12030055, 2020.