2018 42nd IEEE International Conference on Computer Software & Applications

A privacy safeguard framework for a WebRTC/WoT-based healthcare architecture

Saad EL JAOUHARI and Ahmed BOUABDALLAH
{saad.eljaouhari, ahmed.bouabdallah}@imt-atlantique.fr
IMT Atlantique, IRISA, UBL, F-35576 Cesson Sévigné, France)

***Abstract*—In this paper, an e-health architecture offering secure remote medical services using WebRTC (Web Real-Time Communication) enhanced with contextual health information coming from medical connected sensors, is proposed and analyzed. The goal is to allow patients (injured, elderly, disabled, etc.) to benefit from a medical assistance just by calling a remote medical support (doctors, nurses, etc.) using a real-time communication technology such as WebRTC. Moreover, the advancement of the medical devices, on one side, and the emergence of the Web of Things (WoT), on the other side, makes this approach possible. Hence, granting the users the ability of monitoring their own health status and an awareness of their health condition. However, in such architectures, in order for the users to access these services, they need to provide and exchange personal data, and in particular the health related ones. Therefore, user's private information may be exposed to privacy violation and disclosure. Understanding the privacy holes regarding the protection of the personal health related data, identifying the privacy leakage points and studying the privacy requirements are important in order to propose a privacy safeguard for the proposed healthcare architecture, which is the aim of this paper. Additionally, a risk analysis, the sources of these risks and the possible countermeasures are also conducted during this process.**

***Index Terms*—WebRTC, WoT, Security, Privacy, GDPR, Privacy Impact Assessment, Risk Analysis.**

I. Introduction

In an aging population where more and more persons need healthcare and continuous medical surveillance, several researches have been conducted to allow everyone to be able to get the necessary medical care, anytime and anywhere. Moreover, with the advancement of the communication technologies, allowing users to communicate in real-time with almost anyone around the globe, opens new opportunities to the researchers to develop new use cases in order to benefit from the real-time advantages. WebRTC overcomes the challenges of converging into a single technology two traditionally opposite sides of the Web represented by the asynchronous client-server paradigm on one hand, and the domain of peer-to-peer multimedia and real-time communications on the other hand. Technically, it allows Web-based applications to exploit dedicate native APIs implemented in the browser. Allowing, hence, a secure exchange of media and data in real time and in a peer-to-peer fashion [1].

In the other hand, statistics show that the number of connected devices is increasing dramatically, where it is estimated to have more than 30 billions connected devices in 2020 [2]. Which also means processing and protecting more and more data. Medical devices for healthcare are also expected to grow rapidly, where it is estimated that in 2020 each house might contain more than 30 devices just for healthcare, according to [3]. With such growth, we can benefit from the advantages brought by the WoT framework, where we can connect any device without the need to worry about the communication capabilities of the other devices [4].

We are particularly interested in the articulation between WebRTC and the WoT, specially in the case of e-health. A new smart health architecture illustrated by several innovative use cases is provided in [5]. However, the large scale deployment of WoT/IoT technologies in e-health requires particular attention to the security and privacy issues. A comprehensive security analysis of this architecture has been conducted where we provide different solutions to take into account the main security requirements : authentication, confidentiality, integrity and access control [6]. We propose in this paper to complete our approach by tackling the privacy issues.

Moreover, privacy is considered as a basic requirement for consumer acceptance of any kind of services that uses personal data, and in particular the health related ones. However, most of the current healthcare architectures do not provide a deep analysis of the privacy issues, which may lead to privacy breaks in the future. This paper aims at analyzing the privacy leakage issues regarding the remote health services provided by our proposition, and building a privacy safeguard framework in order to ensure the respect of the principle of the "privacy by design". The privacy analysis should be done all along the life cycle of the personal data, from the owner to the final destination and afterward. Privacy requirements should be then implemented within the architecture by including the security countermeasures

0730-3157/18/$31.00 ©2018 IEEE
DOI 10.1109/COMPSAC.2018.10278

required by the privacy analysis.

In the rest of this paper, a special focus will be given to the privacy analysis of our proposed WebRTC-WoT-based e-health architecture. To the best of our knowledge, currently there is no privacy analysis and privacy safeguard proposition of such architectures, and most of them just mention it as a requirement. The remainder of the paper is organized as follows: in II, the global architecture and the analyzed use cases will be presented. In III, a state of the art of the related works is presented. In IV, a comprehensive privacy analysis, based on a set of regulations and new laws is provided. And finally in V, a conclusion with a resume.

II. Architecture

Globally, as explained in [5], the objective is to allow patients to communicate remotely with a medical assistance (which can be doctors, nurses, etc.) in real-time, and to provide them with the capability of exchanging/sharing their medical data with the medical assistance. These medical data can be either medical records/document, or it can be medical data freshly generated by some medical sensors. We are particularly interested in the second case. We decided to use WebRTC as a communication protocol [1].

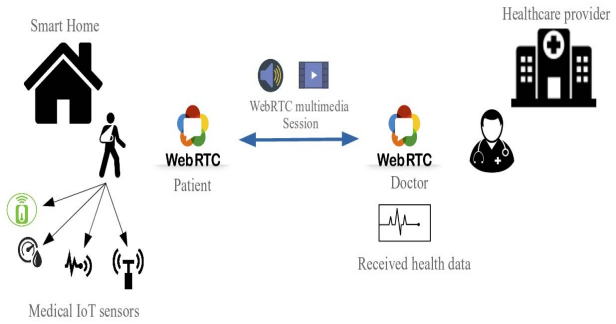

Fig. 1: Tele-consultation service

As shown in Fig.1, the idea consists in accessing the medical sensors, and to send these data to the other side of the communication in real-time during a WebRTC multimedia session. This enables us to create new opportunities, since in this case, we consider that each WebRTC endpoint is a gateway to its own medical Things. In this paper, we are particularly interested in the context of the next generation telemedicine services, that can be divided into several types:

Tele-consultation: where the patient speaks with the doctor remotely using an audio/video system while sending health data coming from medical IoT sensors.

Telemetry: where patients equipped with medical sensors (such as a holter, alarm from from artificial heart, etc.) can be monitored either inside a hospital or remotely, and in the case of an anomaly, an alert is sent to the corresponding caregiver.

Tele-expertise: doctors exchange expertises for a particular case of a patient.

The privacy analysis will focus on the tele-consultation use case, where critical and sensitive medical data is transiting in real-time between the doctor and the patient, and the goal is to be able to identify the different privacy risks inside the architecture and try to mitigate them by providing a set of countermeasures.

Tele-consultation scenario description

The process is described in the following figures:

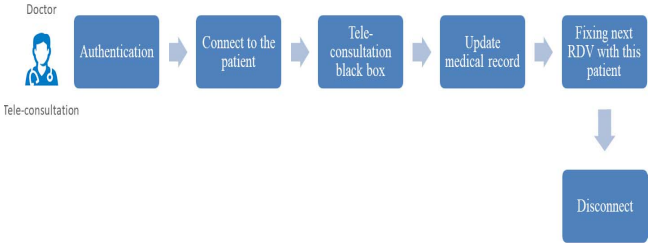

Fig. 2: Tele-consultation from the doctor side

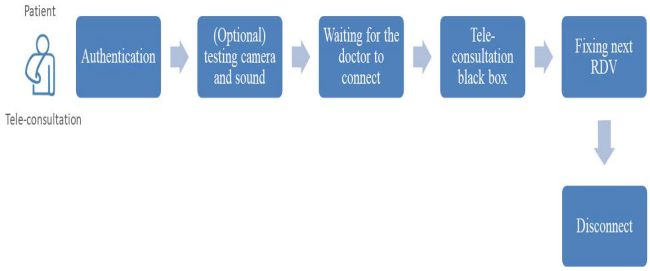

Fig. 3: Tele-consultation from the patient side

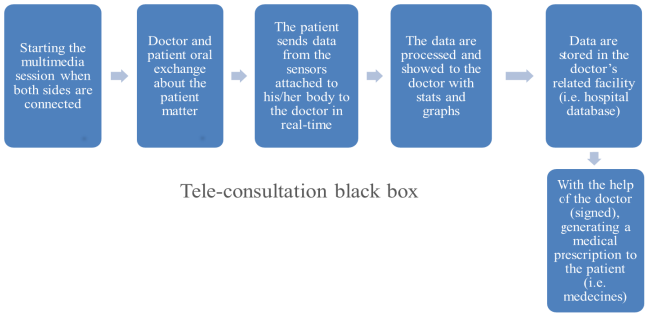

Fig. 4: The Tele-consultation black box

III. Related work

The literature provides several solutions for e-health services, in particular for the remote monitoring service. [7] builds an Android mobile application for the healthcare services, which uses the idea of Internet of Things (IoT) and cloud computing. The application provides the end user with visualization of their Electro Cardiogram (ECG) waves and data logging. The only security aspect that they deal with is the encryption of the medical data and the secure upload to the cloud. However, they lack the privacy aspects and the analysis of the other security issues. In [8], the authors provide an interactive telecare system (ITCS) particularly designed for diabetic patients, providing interaction with caregivers in order to increase self-care quality by adopting IoT. Also, their system enables direct communication between patients medical devices (in particular the blood glucose monitor) and their caregivers smartphone. However, the only security aspect that they deal with is the encryption (using AES) of the transmitted medical data from the ITCS to the cloud. Hence, the privacy aspects and the other security issues are not mentioned. In [9], the authors discuss how to build an ad-hoc extensible healthcare remote monitoring system by using low cost wireless sensors and already existing Internet of things technology as a communication platform. The system alerts, in real time, patients' relatives or medical doctors in case of detection of an abnormality for elderlies. However, they do not provide neither a security nor a privacy analysis of their proposition. Moreover, other system presenting innovative and new ways for health monitoring are present in [10] [11] [12] [13] and in [14]. However, none of them consider the privacy issues regarding the personal health data, which can be an obstacle toward the adaptation of these solutions. This paper [15], provides a privacy analysis of healthcare services in the smart city, and how the data's privacy should be protected while interconnecting the different entities. They propose a privacy engineering approach and safeguard framework are proposed for smart city healthcare services. They analyzed the privacy of the data for a particular use case of "Smart in-Home Emergency Health Service", and they identified the privacy requirements. However, the work presents only a theoretical study, with high level privacy instructions in order to evaluate the privacy of any use case.

Previously in [5], an e-health architecture, with well developed use cases is presented, together with a deep security analysis of the different layers in [6]. Compared to the related works, and in addition to the already implemented security layer, a well defined privacy analysis especially suitable for the next generation telemedicine services is provided. Also, particular interest is given to the personal health data protection issues and to the different rights of the patient in our architecture. Finally, and with the help of the privacy impact assessment (PIA)[16], a risk analysis is provided, together with the countermeasures to mitigate them.

IV. Privacy analysis

A. Regulations

In order to conduct the privacy analysis, several regulations and frameworks have been studied in order to have a global view of the privacy requirement for the health related personal data, and we mention:

- The analysis of the European GDPR laws in [17]
- The use of the French Privacy Impact Assessment (PIA) framework [16]
- The European Working Party 223 [18]
- The French regulation regarding the personal health data, through ASIP [19]

Hence, these regulations and frameworks will be used in order to understand the privacy weaknesses regarding the protection of the personal health related data, to identify the privacy leakage points and to study the privacy requirements, in order to propose a privacy safeguard for the proposed healthcare architecture. Additionally, a risk analysis, the sources of these risks and the possible countermeasures are also conducted during this process.

B. Data protection principles and user's rights

According to the GDPR law [17], the main principles that need to be applied to the personal data, and in particular to health related one, and that need to be always respected by the data controllers, are:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Limited storage
- Integrity and confidentiality
- Accountability

In such health related architectures, the controller of the data holds several responsibilities in order to protect the data going through the platform, which are mainly, but not limited to:

- Confidentiality and data integrity.
- Secure data storage.
- Anonymity of the data

- Controller access to these data.
- Sending data through secure channels.

Moreover, under the new GDPR laws, the main principles and rights that need to be respected in our architecture, and guaranteed to the patient (data process), are:
The right to access: can be granted to the patient, by allowing him/her to access their medical records through the platform, by a health professional or an equivalent. Also, depending on the age and the mental state of the patient.
The right to portability: in order to mitigate and transfer all the records related to the patient in the database in a standards format, which can be then integrated by any other entity chosen by the patient, an option must be implemented for the last version of the architecture.
Right to rectification or erasure: should be requested to the medical support, for instance regarding the medical record.
The right to be forgotten: upon valid request of the patient, all the related personal data must be erased from the database. This part is guaranteed by the medical service and not the platform, hence out of our scope.
The rights to be informed in case of a breach: where the concerned persons need to be informed as soon as possible. In our architecture, it can be done through an alert or a notification.
The right to be informed/transparency: where the information should be as clear and simple as possible, and in the native language of the patient. Also, this part is provided by the medical service and not the platform, since the medical records are stored in the health infrastructure database, hence out of our scope. However, the user can request the architecture to provide a visualization of the medical data collected by the medical sensors.

C. Assets: personal health data protection

The collected data will be mainly the patients related data (i.e. vital signs such as Body Temperature, Pulse Rate, Respiration Rate, Blood Pressure, etc.) collected via IoT medical sensors attached to his/her body. The only persons that have the right to access these data are: the concerned patient, the related doctors, the health infrastructure where the doctor works, the administrator of the database, government and researchers. For the last three destinations, special consent needs to be provided by the patient.

In this architecture, the life cycle of the health data is described in Fig. 5:

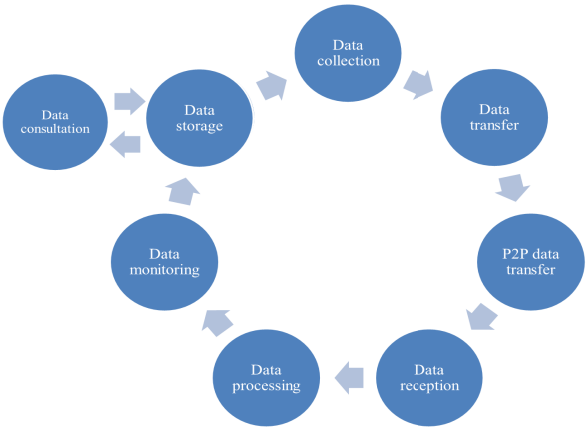

Fig. 5: The health data lifecycle within the architecture

Data collection: medical data (vital signs) are collected from the patient using attached medical body sensors.
Data transfer: data are sent from the sensors to the platform.
P2P data transfer: data are transferred to the remote peer (i.e. the doctor) using a secure WebRTC channel.
Data reception: ensuring the reception of the medical data from the remote peer (i.e. doctor) side.
Data processing: data are processed using for example machine learning in order to evaluate the health data and perform a first analysis in order to detect anomalies.
Data monitoring: the result of the processed data will be shown to the doctor (i.e. graphs).
Data storage: the received data will be stored in the database of the remote peer (it can be the database of the doctor, or a secure provided database, or in the facility where the doctor is -i.e. the hospital-).
Data consultation: the authorized parties can access these medical data anytime through the database.

As for the duration of the processing of such data, it depends on each step of the tele-consultation process. Since the main purpose of our architecture is to perform medical tele-consultations, telemetry and tele-expertise, we consider the collected data as medical records for the patient. The law defines the duration of conservation of lifetime plus 6 years for computerized/electronic medical records. And this is applicable for our architecture in the case if the data is stored in our database. However, if the data is stored in a hospital, this regulation should be applicable in the database of the hospital. The architecture do not store the data during the life cycle of the health data, since the data are sent in real-time to the remote peer. In case the data is stored in the platform, mechanisms for controlling the access and for suppressing data at the end of their

retention period are deployed.

D. Personal health data protection requirements

In this architecture, in order to make the processing of the personal health data licit, several requirements need to be respected, and we mention:
* The explicit consent of the patient in order to use their health data coming from the medical body sensors.
* The explicit consent of the patients when sending their data to the remote medical support (i.e. doctor)
* The explicit consent of the patient in order to use his/her personal health data for research purpose
* The explicit consent of the patient to the doctor in order to transfer his/her data to another medical entity (i.e. to another specialist)
* The processing of the health data of the patient is necessary in order to evaluate his/her health status by the remote medical support. Under the juridical law, the processing is necessary to safeguard the vital interests of the data subject (patient) or other natural person.

E. Security countermeasures and risk analysis

In this light, several security countermeasures need to be implemented in the architecture such as:
Encryption: by using HTTPS and CoAP-DTLS, all the data flow in the architecture are encrypted. Mainly, the data must be peer-to-peer encrypted, from the patient's sensors to the doctor's interface or database.
Anonymity: for research and remote expertises purposes, and after an explicit consent of the data subject (the patient), the data should be anonymized in order to protect the privacy of the patient.
Data minimization: where only the strictly needed data should be collected and processed during teleconsultation process.
Website protection: by securing the website using X.509 certificates, provided by a certificate authority, by using a strong authentication mechanisms such as using OAuth, and by applying the appropriate access control mechanisms.
Integrating the privacy in the design process of the architecture: which is the main aim of this paper, by building a privacy safeguard framework, and analyzing the privacy risk regarding the health data, and to apply the results on the final design of the architecture.
Controlling the access to the health data: an unauthorized access to the resources may cause the loss of confidentiality, integrity, and availability of the resources. Hence, authenticating the users and restricting the access to only the authorized users is required.
Integrity: by maintaining and insuring the accuracy and the consistency of, data over its entire life-cycle, in particular during the transmission, the processing and the storage of these personal data. Unfortunately, data can be compromised in several ways: transfer errors, bugs, malwares, hacked, etc. Hence, mechanisms guaranteeing that the data is intact and unaltered should be implemented using cryptographic algorithms, such as error checking and validation methods.
Confidentiality: in order to prevent sensitive health data from being disclosed to the wrong and unauthorized persons, while making sure that the authorized ones can access it.
Secure storage: by implementing a tiered data protection and security model, applying both logical (authorization, authentication, encryption and passwords) and physical (restricted access and locks on server, storage and networking cabinets) security of the database, in particular in case of health data.
Archiving: the Health Information Portability and Accountability Act (HIPAA) [20] requires health service providers to store theses information for years, sometimes decades. Several options can be considered for the data archiving strategy, it can be ranging from on-site tiered storage within a storage area network (SAN) to off-site storage with an external outsourced regulated service provider. However, security must be given a priority regarding the sensitivity of the data.

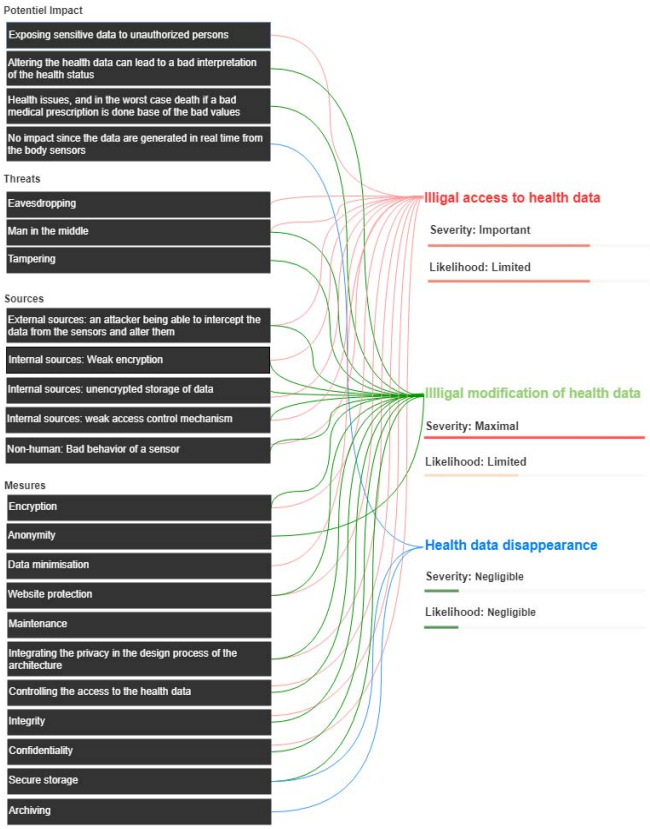

Fig. 6: Global view of the risk analysis

A global view of the privacy risks, together with the potential impact on the personal data, the threats that may trigger the risk, the sources of the risk and the possible measures to counter them (represented by the same color), are presented in the Fig. 6. Risk analysis considers the overall architecture, including the communication system and all the exchanged data.

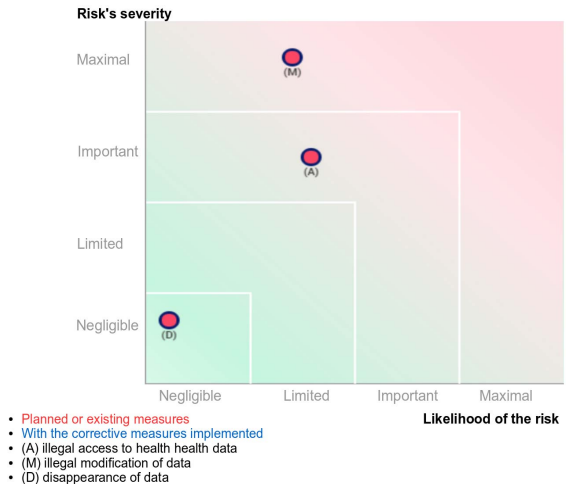

Fig. 7: Risk cartography

The Fig. 7 represents the risks generated by the treatment and the residual risks taking into account all the corrective measures. It demonstrates that if the complementary measures described in the action plan are properly implemented, the likelihood and/or severity of the residual risks should be reduced.

V. Conclusion

In health related services and in particular in telemedicine ones, safeguarding the privacy of the users is as important as the delivery of quality services. Indeed patients are very careful about their personal data. Hence, providing privacy guarantees for protecting these sensitive data is an essential aspect of any medical service in particular the telemedicine one. In this paper, we analyzed the privacy of our telemedicine architecture, in conformance with the GDPR laws, and we identified its weaknesses together with the necessary actions to protect these sensitive data from any privacy threats. We also took into account the users perspectives which are very important in order to identify the privacy requirements in accordance with their expectations and concerns. We showed that our architecture already ensures all the countermeasures except archiving, secure storage, data minimization and anonymity, which we will tackle in our future works. Hence, to be compliant with the privacy by design principle, these missing countermeasures will be integrated in the design plan and in the implementation of this architecture, by following the principles explained in [6].

References

[1] C. Jennings, T. Hardie, and M. Westerlund, "Real-time communications for the web," *IEEE Communications Magazine*, vol. 51, no. 4, pp. 20–26, 2013.

[2] "Internet of things (iot) connected devices installed base worldwide from 2015 to 2025 (in billions)," 2017. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[3] M. K. Weldon, *The future X network: a Bell Labs perspective*. Crc Press, 2016.

[4] D. Guinard and V. Trifa, *Building the Web of Things*. Manning Publications Co, 2016.

[5] S. El Jaouhari, A. Bouabdallah, J.-M. Bonnin, and T. Lemlouma, "Toward a smart health-care architecture using webrtc and wot," in *Recent Advances in Information Systems and Technologies: Volume 3*, 2017, pp. 531–540.

[6] S. El Jaouhari, A. Bouabdallah, and J.-M. Bonnin, "A secure webrtc/wot-based health-care architecture enhanced with access control," in *The 32nd International Conference on Information Networking (ICOIN) 2018, Chiang Mai, Thailand (accepted)*.

[7] J. Mohammed, C. H. Lung, A. Ocneanu, A. Thakral, C. Jones, and A. Adler, "Internet of things: Remote patient monitoring using web services and cloud computing," in *2014 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom)*, Sept 2014, pp. 256–263.

[8] S. J. Wu, R. D. Chiang, S. H. Chang, and W. T. Chang, "An interactive telecare system enhanced with iot technology," *IEEE Pervasive Computing*, vol. 16, no. 3, pp. 62–69, 2017.

[9] F. Jimenez and R. Torres, "Building an iot-aware healthcare monitoring system," in *34th International Conference of the Chilean Computer Science Society (SCCC)*, Nov 2015.

[10] A. M. Ghosh, D. Halder, and S. K. A. Hossain, "Remote health monitoring system through iot," in *2016 5th International Conference on Informatics, Electronics and Vision (ICIEV)*, May 2016, pp. 921–926.

[11] M. S. D. Gupta, V. Patchava, and V. Menezes, "Healthcare based on iot using raspberry pi," in *International Conference on Green Computing and Internet of Things (ICGCIoT)*, Oct 2015.

[12] H. N. Saha, S. Auddy, S. Pal, S. Kumar, S. Pandey, R. Singh, A. K. Singh, P. Sharan, D. Ghosh, and S. Saha, "Health monitoring using internet of things (iot)," in *8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)*, Aug 2017, pp. 69–73.

[13] M. S. Mahmud, H. Wang, A. M. Esfar-E-Alam, and H. Fang, "A wireless health monitoring system using mobile phone accessories," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2009–2018, Dec 2017.

[14] S. S. Al-Majeed, I. S. Al-Mejibli, and J. Karam, "Home telehealth by internet of things (iot)," in *2015 IEEE 28th Canadian Conference on Electrical and Computer Engineering (CCECE)*, May 2015, pp. 609–613.

[15] A. A. Alghanim, S. M. M. Rahman, and M. A. Hossain, "Privacy analysis of smart city healthcare services," in *IEEE International Symposium on Multimedia (ISM)*, Dec 2017.

[16] "Les pia (privacy impact assessment)." [Online]. Available: https://www.cnil.fr/fr/PIA-privacy-impact-assessment

[17] "General data protection regulation (gdpr)," April 2016. [Online]. Available: https://www.eugdpr.org

[18] P. O. P. DATA, "Article 29 data protection working party," 2014.

[19] ASIP, "l'agence franaise de la santé numérique." [Online]. Available: esante.gouv.fr

[20] A. Act, "Health insurance portability and accountability act of 1996," *Public law*, vol. 104, p. 191, 1996.