2020 The 3rd World Symposium on Communication Engineering

An Efficient IoT System Respecting the GDPR

Chrysi Metallidou, Konstantinos E. Psannis, Eugenia Alexandropoulou-Egyptiadou
Department of Applied Informatics
University of Macedonia
Thessaloniki, Greece
e-mails: chrysi.metallidou@gmail.com, kpsannis@uom.edu.gr, ealex@uom.edu.gr

***Abstract*—Smart technologies integrated in the industry of Hotels is an emerging field in terms of the revolution of industry 4.0. Hotels in the context of providing luxury, specialization, intelligence and easiness to the residents, regarding the hotel's services, are willing to transform their concept into smart hotels by applying the Internet of Things (IoT) technologies to every operation, device, functionality and service and by providing to the residents the convenience of handling everything simply on themselves, through a smart device. However, security features of the IoT applications and privacy for the users are great issues for users and Organizations (residents and the industry of Hotels), due to the General Data Protection Regulation (GDPR).In this paper, we focus on the development of a smart system, than can be applied to any smart building, especially to an intelligent hotel, that supports all smart functionalities, provides the desired convenience to the users, bases on IoT technologies and takes into account security and privacy preconditions indicated by the GDPR.**

Keywords-IoT technology; smart technology system; secure operation; smart hotel; privacy to user; GDPR

I. INTRODUCTION

This era is characterized by technological advances which serve the international community and aim to provide value and quality to the life of its residents. Prosperity, intelligence, simplicity and efficiency are concepts that the achievements of the Internet of Things technology, have managed to provide to the industry and the users.

An IoT system consists of an internet connection among sensors and devices and information from the physical world is obtained and automated, specified actions are performed back to the physical world. From this functionality derive security and privacy concerns for internet applications due to IoT systems', cloud based architecture on which data may be stored or be exchanged, see Fig.1. A survey from the literature on the security of commercial IoT frameworks [1], such as AWS IoT, SmartThings, Azure IoT, has indicated that they are secure in case that they are developed under security features. On the other hand, the data provided though IoT devices and their utility has motivated the largest technology companies in the world [2] to expand the demand for more innovative IoT devices.

In a smart hotel, the Internet of Things (IoT) consists of smart sensing technologies, smart devices, services and technical systems connected to network. In a smart hotel, with the aim to achieve speed, quality and comfort, a smart management system should be developed, that provides intelligent and automated control with self-awareness, self-prediction, self optimization, self-configuration and self-diagnosis.

In addition, a smart hotel should respect the privacy of the users, their right to erase their personal data and preferences, after leaving hotel and should also provide security in their transactions and in their online options, when using the smart system. In other words, a smart hotel's operations should be in compliance with the General Data Protection Regulation (GDPR), which is mandatory and valid for all European Member States. Its purpose is to harmonize data privacy laws across Europe, to protect the personal data of all European citizens [3] and to comply with data privacy, the actions of all organizations. In the context of the fact that personal data are distributed through Smart Cities, E-business, E-government, the GDPR is vital for the further development of a secure digital economy [3].

This paper is organized as follows; section II presents a report of the related work that has been conducted regarding privacy and security in IoT systems. Section III provides the GDPR and the security requirements for a smart hotel system, section IV presents the development of the smart system and its functionality, basing on IoT technology and section V provides the conclusions.

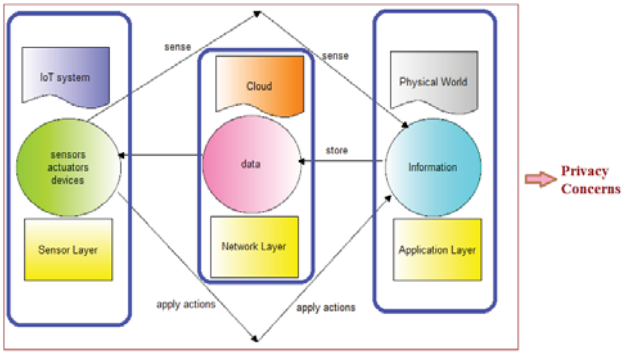

Figure 1. IoT architecture and privacy concerns.

II. RELATED WORK

For the purpose of this study we review and analyze previous literature which has been published in the fields of smart cities and security, IoT and privacy, in order to collect all representative information for the development of a smart

978-1-7281-8564-4/20/$31.00 ©2020 IEEE

hotel's secure IoT system. The methodology we follow complies with the GDPR.

The following paragraphs present the papers which contributed significantly in our study. To begin with the topic of IoT and smart cities in [4],[5],[6], the authors discuss the application of the GDPR in the development of the smart cities' technologies and specifically IoT technology. The point is that since smart cities deals with people that live, act and trade, the collection of their personal data through IoT systems is inevitable. Therefore, the authors analyze the way legal principles can be supported in a layered IoT architecture, so as to meet the privacy requirements for users and IoT systems. Consequences of the GDPR in case an organization will not comply with it and the way that organizations and enterprises should adjust their operation to the GDPR, so as to avoid data breach and penalty, is also stated in [6].

In [7], a survey is conducted regarding the awareness of international students on privacy issues related to the usage of IoT-Fog-Cloud systems and AI solutions. According to the results of the survey, the authors state proposals for secure utilization of IoT systems.

In [8],[9],[10],[11] the authors develop security IoT environments for smart cities. In [8], a smart Governance environment is developed regarding governance and management challenges of heterogeneous IoT systems that serve smart cities. The goal of the proposed system is to provide a range of functionalities, customized for use by each smart city. In [9] and [10], the authors focus on Snap4City solutions regarding architecture and components that enable the platform to comply with security standards and the GDPR. In [11], is presented a design of a process for consent of personal information collection that meets the legal conditions of privacy policy and can be integrated in an IoT system that satisfies the consent requirements of GDPR. In [12], the authors propose a framework for information and consent in the IoT to secure data subjects and data controllers. Requirements for information and consent and several technical solutions to implement them are presented and also a prototype is implemented.

The paper in [13], refers to current issues of individual privacy in the healthcare domain that stem from IoT technology devices. In [14], the authors propose a solution of a GDPR Controller in IoT systems. The solution gives the data owner a full control of his data and the controller architecture is validated and evaluated using an e-health case.

III. Security Requirements for an IoT System

A. Type of Circulating Personal Data in the IoT System

In the literature [17] it is stated that in the last two years the 80% of the international online data, was created. In parallel the use of IoT devices contributed in the direction of increasing the amount of data that are collected and processed and further the integration of Artificial Intelligence into this data, increased their appraised value and triggered the targeted and custom advertisements for commercial and profitable purposes[18][19]. As a result, the transparency and accountability of the amounts of data that are generated and transmitted, is questionable regarding the use of these intelligent systems [20]. Further, the process of collecting and processing personal data may seem innocent, but in our days privacy concern is a major issue, because a data combination may result in profile formation and identification of an individual [20]. The type of circulating personal data in the proposed IoT system may be:

- first name, last name, credit card, location
- interests and hobbies, consumer preferences, habits
- phone contacts and emails, day schedule, meetings and dates
- Dietary preferences, light and heat preferences, sleeping patterns and timetables.

Therefore the proposed IoT system should achieve [20]:

- Processing Trust (correct and least required data)
- Connection Trust (exchange the right data with the right services' providers and nobody else)
- System Trust (a trustworthy system that provides transparency)

B. Personal Data and Privacy

The General Data Protection Regulation [15], applies to the processing of personal data by all Union institutions and bodies. Regulation 2016/679, art. 1 and art. 2, protects fundamental rights and freedoms of natural persons, in particular, their right to the protection of personal data, and applies rules relating to the processing of personal data wholly or partly by automated means, regardless of whether the processing takes place in the Union or not art.3. Personal data, according to art.4, par.1, means any information relating to a natural person, which is the data subject, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Processing on personal data, according to art.4 par. 2, means any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Consent of the data subject, according to art.4, par.11, means any freely given, specific, informed and unambiguous indication of the data subject's, wishes by which he or she, by a statement, signifies agreement to the processing of personal data relating to him or her. Electronic communications[1] network [16] means a transmission system, based or not on a

[1]Regulation (EU) 2018/1725, art. 3, par.25, electronic communications network means a transmission system, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio,optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched including internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed

permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment, including network elements, including satellite networks, fixed (circuit- and packet-switched including internet) and mobile terrestrial networks, for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.

In order to ensure privacy and security in an IoT system, we should consider the following requirements mentioned also on Table I. Initially the provider of a secure IoT system should apply data minimization by requiring from a natural person only the necessary data for process and should store those data for the minimum time required. In addition the provider should define who has accessibility to those personal data and should integrate in the IoT system a way for the data subject to give or withdraw consent for his/her personal data process. The IoT system should also integrate a way for the data subject to correct his/her personal data or erase them from the system after communication with the IoT system is completed. The provider of the IoT system is also responsible for maintaining records of processing activities. Last but not least, the IoT system should ensure security of personal data and security of processing by applying pseudonymisation or encryption of personal data, by ensuring confidentiality, integrity, and resilence among the processing system and services, by considering access to personal data in a timely manner in the event of a physical or technical incident and by applying testing to evaluate the effectiveness of technical measures that ensure secure processing.

IV. The Development of a Secure IoT System: A Smart Hotel Case

For the proposed IoT system, we need to define the entities involved in the system. Initially, it is a cloud based system which through communication server setups communication among participants and carries out the transfer of user's data. There exist 1) Things: smart devices, sensors/actuators, services/facilities. The communication among Things is allowed according to the Contracts. 2) Users of the system: they are authorized and require for a service or information and are allowed to keep their anonymity. Users can view the facilities and services of the Organization and their actions are restricted to service. 3) Organization: owns and handles the management of the IoT system through a manager, the manager takes care for the functionality of the system. 4) Contracts: are created for achieving a privacy exchange of data among devices or services and services, Contracts are a mean to authorize Things, a Contract can be cancelled either when a service is completed or when the user departs.

TABLE I. Requirements for an IoT System under Considering Personal Data Protection

1.Data protection by design, 2016/679	Art. 25, par.1 data minimisation	Art 25, par.2, personal data: purpose limitation, storage limitation, accessibility
2.Consent 2016/679	Art.6 data subject can give or withdraw consent for personal data process	
3.Rectification/ Erasure, 2016/679	Art. 13 data subject has the right to correct inaccurate personal data	Art.14 data subject has the right to obtain erasure of personal data
4.Records, accountability, 2016/679	Art. 30 each controller[2] shall maintain records of processing activities	
5.Security, 2016/679	Art. 32, security of personal data and security of processing them	a)Pseudonymisation, encryption of personal data, b)confidentiality, integrity, availability and resilence of the processing systems and services, c)restore availability and access to personal data

The operations that are provided to the system can refer to the adjustment of the technical systems of a building such us lightening, heating, ventilation, air conditioning or to order/buy things, book reservations in spa or restaurants or handle meetings, calls, messages, emails and music, require services and information or anything else the Organization is willing to provide. In the functionalities of the system is also enlisted the local storage of records with personal data for a minimum period of time, specified by the Organization.

The hardware features of the IoT system includes building sensors and actuators such us occupancy sensors, servo-motors, smart appliances, smart phones and a Raspberry Pi that enables sensor data circulation. To continue with the framework of the IoT architecture, it includes 3 Layers: Sensor Layer, Network Layer and Application Layer [21], in each of which we should apply security mechanisms to achieve privacy by design. In the Application and Network Layer we need to authenticate the users that connect to the system. In the proposed management system the manager introduces the minimum personal data of the users and then the users, in order to access the system, they have to verify and give consent for the process of their personal data or rectify personal data. Then, for using all services and facilities they have to sign in, by introducing to the system a username and a password, so as to ensure pseudonymisation of the users, as well. Afterwards, the management system will authorize the users to access the system, which is a very important feature of privacy, due to the large amount of devices, services and people that use the same network of the IoT architecture. Further, in the Application and Network Layer, we should ensure that the moment an authorized user requires a service or information, the data are available and the exchange of

[2] Regulation (EU)2016/679, art.4, par.7,controller 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law

data is carried out. In addition, in the Network Layer, we should ensure trustworthy among IoT nodes and avoid malicious actions.

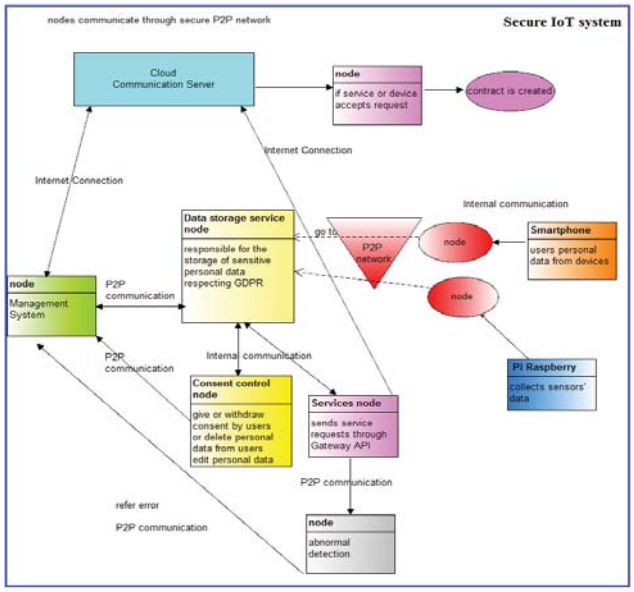

Figure 2. Implementation of the IoT system.

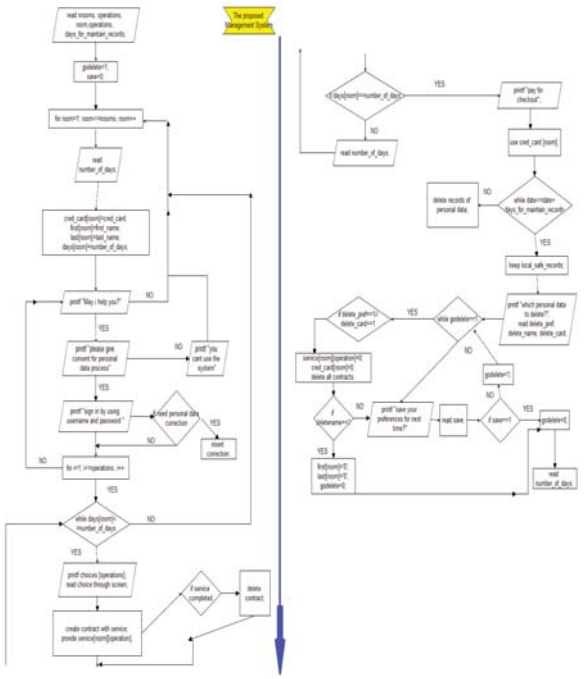

Figure 3. Flow chart of the proposed system.

The architecture of the system is implemented through nodes which communicate through peer to peer (P2P) network. The nodes has gateway API which performs the P2P communication and enables in cooperation with the Communication Server, the Contract creation for a service. The data collected from sensors and from user are gathered from the Data Storage Service to apply consent control. The management system promotes an IoT request for a service and if the provider accepts the request, the Contract is created. Every time a communication request appears between 2 Things, the API Gateway is used to require from the Communication Server permission or denial, according to the Contracts, for the communication request. Fig.2 illustrates the implementation of the IoT system and Fig.3 presents the flow chart of the management system's functionality and interaction with the user.

V. CONCLUSION

In this paper we implemented and presented an IoT system that can offer to the clients of an Organization intelligence, convenience and easiness by utilizing technology and incorporating the latest technological advances in its functionality. Simultaneously, the proposed IoT system considers privacy and security preconditions and complies with the GDPR. Specifically, it provides Data protection by design requires consent to personal data process from the data subject, enables rectification of personal data and the right to be forgotten by erasure of personal data. Furthermore, this IoT system maintains records of processing activities for a minimum time, enables accountability and achieves security of processes by using pseudonymization, as well. Our future target is the integration of this IoT system into the interoperability of a hotel in order to monitor the functionality of the system and the guests' behavior.

REFERENCES

[1] M. Ammar, G. Russello, and B. Crispo, "Internet of things: A survey on the security of iot frameworks," Journal of Information Security and Applications, vol. 38, pp. 8–27, 2018

[2] Lσpez G., Quesada L., Guerrero L.A. "Alexa vs. Siri vs. Cortana vs. Google Assistant: A Comparison of Speech-Based Natural User Interfaces". In: Nunes I. (eds) Advances in Human Factors and Systems Interaction. AHFE 2017. Advances in Intelligent Systems and Computing, vol 592. Springer, Cham, 2018

[3] G. Vojkovic, "Will the GDPR slow down development of smart cities?," *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, 2018, pp. 1295-1297, doi: 10.23919/MIPRO.2018.8400234.

[4] C. Li and B. Palanisamy, "Privacy in Internet of Things: From Principles to Technologies," in IEEE Internet of Things Journal, vol. 6, no. 1, pp. 488-505, Feb. 2019, doi: 10.1109/JIOT.2018.2864168

[5] S. Varadi, G. G. Varkonyi and A. Kertesz, "Law and IoT: How to see things clearly in the Fog," 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC), Barcelona, 2018, pp. 233-238, doi: 10.1109/FMEC.2018.8364070

[6] G. Priyadharshini and K. Shyamala, "Strategy and Solution to comply with GDPR : Guideline to comply major articles and save penalty from non-compliance," 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on, Palladam, India, 2018, pp. 190-195, doi: 10.1109/I-SMAC.2018.8653696.

[7] G. G. Varkonyi, A. Kertesz and S. Varadi, "Privacy-awareness of Users in our Cloudy Smart World," 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC), Rome, Italy, 2019, pp. 189-196, doi: 10.1109/FMEC.2019.8795310.

[8] A. Kazmi, M. Serrano and A. Lenis, "Smart Governance of Heterogeneous Internet of Things for Smart Cities," 2018 12th International Conference on Sensing Technology (ICST), Limerick, 2018, pp. 58-64, doi: 10.1109/ICSensT.2018.8603657.

[9] C. Badii, P. Bellini, A. Difino and P. Nesi, "Smart City IoT Platform Respecting GDPR Privacy and Security Aspects," in IEEE Access, vol. 8, pp. 23601-23623, 2020, doi: 10.1109/ACCESS.2020.2968741.

[10] C. Badii, P. Bellini, A. Difino and P. Nesi, "Privacy and Security Aspects on a Smart City IoT Platform," 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Leicester, United Kingdom, 2019, pp. 1371-1376, doi: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00250.

[11] G. Y. Lee, K. J. Cha and H. J. Kim, "Designing the GDPR Compliant Consent Procedure for Personal Information Collection in the IoT Environment," 2019 IEEE International Congress on Internet of Things (ICIOT), Milan, Italy, 2019, pp. 79-81, doi: 10.1109/ICIOT.2019.00025.

[12] V. Morel, M. Cunche and D. Le Métayer, "A Generic Information and Consent Framework for the IoT," 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 2019, pp. 366-373, doi: 10.1109/TrustCom/BigDataSE.2019.00056.

[13] R. Alharbi and H. Almagwashi, "The Privacy Requirments for Wearable IoT Devices in Healthcare Domain," 2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Istanbul, Turkey, 2019, pp. 18-25, doi: 10.1109/FiCloudW.2019.00017.

[14] M. Rhahla, T. Abdellatif, R. Attia and W. Berrayana, "A GDPR Controller for IoT Systems: Application to e-Health," 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Napoli, Italy, 2019, pp. 170-173, doi: 10.1109/WETICE.2019.00044.

[15] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of natural persons with regard to the processing of Personal Data and on the Free Movement of such Data and repealling Directive 95/46/EC (General Data Protection Regulation) [Online]. Available: https://www.eurlex.europa.eu/eli/reg/2016/679/oj

[16] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1592491393870&uri=CELEX:32018R1725

[17] Vishal, K., "Big Data facts", https://analyticsweek.com/content/big data-facts/, August 2017

[18] Goksel Canbek, N., Mutlu, M., "On the track of Artificial Intelligence: Learning with Intelligent Personal Assistants", Journal of Human Sciences, vol 13, no1, 2016

[19] Biljana, L., Risteska, S., Trivodaliev, KV., "A review of Internet of Things for smart home: Challenges and solutions", Journal of Cleaner Production,Volume 140, Part 3,Pages 1454-1464, 2017.

[20] E. Furey and J. Blue, "Can I Trust Her? Intelligent Personal Assistants and GDPR," 2019 International Symposium on Networks, Computers and Communications (ISNCC), Istanbul, Turkey, 2019, pp. 1-6, doi: 10.1109/ISNCC.2019.8909098.

[21] M. Koutli et al., "Secure IoT e-Health Applications using VICINITY Framework and GDPR Guidelines," 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini Island, Greece, 2019, pp. 263-270, doi: 10.1109/DCOSS.2019.00064.