2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)

Security Challenges in the eHealth Domain: The VICINITY Approach

Maria Belesioti[1*], Evangelos Sfakianakis[1], Viktor Oravec[2], Athanasios Tryferidis[3], Kostis Kaggelides[4], Ioannis P. Chochliouros[1], Maria Koutli[3] and Dimitrios Tzovaras[3]
[1]Hellenic Telecommunications Organization S.A. (OTE), Fixed Network R&D Programs Section, Athens, Greece
{mbelesioti, esfak, ichochliouros}@oteresearch.gr
[2]bAvenir, s.r.o., Bratislava, Slovakia (viktor.oravec@bavenir.eu)
[3]CERTH/ITI - Centre for Research and Technology Hellas/Information Technologies Institute, Thessaloniki, Greece
{thanasic, mkoutli, dimitrios.tzovaras}@iti.gr
[4]Gnomon Informatics S.A., Thessaloniki, Greece (k.kaggelides@gnomon.com.gr)

***Abstract*—The eHealth constitutes the largest wave of change in the sector of healthcare. In this context, Internet of Things is of immense importance since connected data would facilitate treatment with more efficiency and comprehensive knowledge and would "act" as preventive medicine. Monitoring health data and making them ubiquitously accessible to predefined and authorized healthcare personnel are shared through various IoT platforms, which usually lack IoT-protocol-interoperability. In this paper, we present the impact of IoT systems in the eHealth services' evolution and we introduce the VICINITY ecosystem solution. Its high-level architecture is analyzed and several security considerations are offering "thought for food".**

Keywords— Internet of Things (IoT), healthcare, eHealth, interoperability, decentralization, assisted living

I. INTRODUCTION

The most important advantage of today's growing technology investments should be adopted to make living smarter and more e-centric. It is anticipated that more than 75 billion devices will be connected to the Internet of Things (IoT) by 2020 [1] and that billions of sensors and actuators will be connected to the Internet via heterogeneous access networks enabled by modern technologies such as real-time and semantic web services. The Internet of Things is envisioned to allow interconnectivity of anyone and at anytime and anyplace assisting, at the same time, our interaction with the environment by linking the web with different wearables and working devices such as medical devices.

The IoT concept was coined by a member of the Radio Frequency Identification (RFID) development community in 1999, and it has recently become more relevant to the practical world because of the growth of mobile devices, embedded and ubiquitous communication, cloud computing and data analytics [2]. Nowadays, IoT is been applied in areas such as home monitoring and automation, healthcare, energy and utilities, smart grid, intelligent transportation systems and traffic management. Regarding healthcare, the use of IoT could be particularly useful due to the recent advances of information and communication technologies and can have great impact to both remote monitoring of patients and preventive medicine sectors. More specifically, eHealth applications are of high interest due to their capability to improve accessibility with parallel reduction of healthcare cost and, *most importantly*, without discounts in the quality of life of patients. Easy, quick and secure access to quality healthcare services is important for increasing everyone's quality of health, preventing disease and disability, detecting and treating health conditions, and maybe preventing death due to time strains. Section II provides a fundamental overview of the essential VICINITY approach, by briefly discussing the proposed high-level architecture, decentralization issues and proposed eHealth use cases. Section III refers to actual IoT challenges in the eHealth environment. Then, section IV focuses upon security considerations affecting the eHealth domain. Section V summarizes the work and predicts for next steps.

II. THE VICINITY APPROACH

VICINITY ("*Open virtual neighbourhood network to connect intelligent buildings and smart objects*") is an H2020 research and innovation project that aims at addressing the challenging objective of an interoperable IoT ecosystem that will allow collaboration of IoT platforms towards the creation of virtual neighbourhoods. This section presents the technical "key points" of the VICINITY concept and the envisioned eHealth use case that will demonstrate the applicability of the proposed solution.

A. High Level Architecture

Current IoT infrastructure acts as isolated islands in the global IoT landscape while inter-connection of these "islands" might bring significant added value (such as an ecosystem running on close-to-zero energy, *for example*). The high-level concept of the VICINITY framework is outlined in Fig.1, *below*. As indicated in the respective figure, guest IoT infrastructures, VICINITY enabled services

2325-2944/19/$31.00 ©2019 IEEE
DOI 10.1109/DCOSS.2019.00057

as well as the VICINITY auto-discovery space, are connected to a VICINITY interoperability gateway using the same VICINITY gateway API (Application Programming Interface).

The VICINITY ontology network will be used throughout the entire VICINITY ecosystem and by the different "actors" that consume the information generated by such systems. The VICINITY ontology will serve as a shared vocabulary and model in the whole project and will be based on current standards, such as the W3C Semantic Sensor Network (SSN) ontology [3].

The open VICINITY interoperability gateway transfers IoT data between two peers in a semantic format derived from the VICINITY IoT ontology that is converted to/from the client formats by the VICINITY Gateway API module. User plane communication can be configured as end-to-end (not routed via the communication server). However, such setup usually requires special firewall configuration. Therefore, user plane routing via server will be made possible. The VICINITY Gateway API will use VICINITY security services for end-to-end encryption and authentication of IoT messages.

and operational services for logging and automated periodic maintenance.

The VNM is acting as the VICINITY user interface that is available for the users, either via standard web browser (including mobile devices) or via web services if the user is intended to integrate its features into its own operational console. The VICINITY neighbourhood manager will be running as a web application on a high available web server and will store the users' authorization rights in the VICINITY user database. The users will be able to share the access to their smart objects with whomever they choose, without losing the control over them[4].

The discovery of IoT objects is driven by the IoT auto-discovery platform, which invokes instances of the VICINITY Agent component to handle the semantic matching between parameterized demands and available IoT node descriptors.

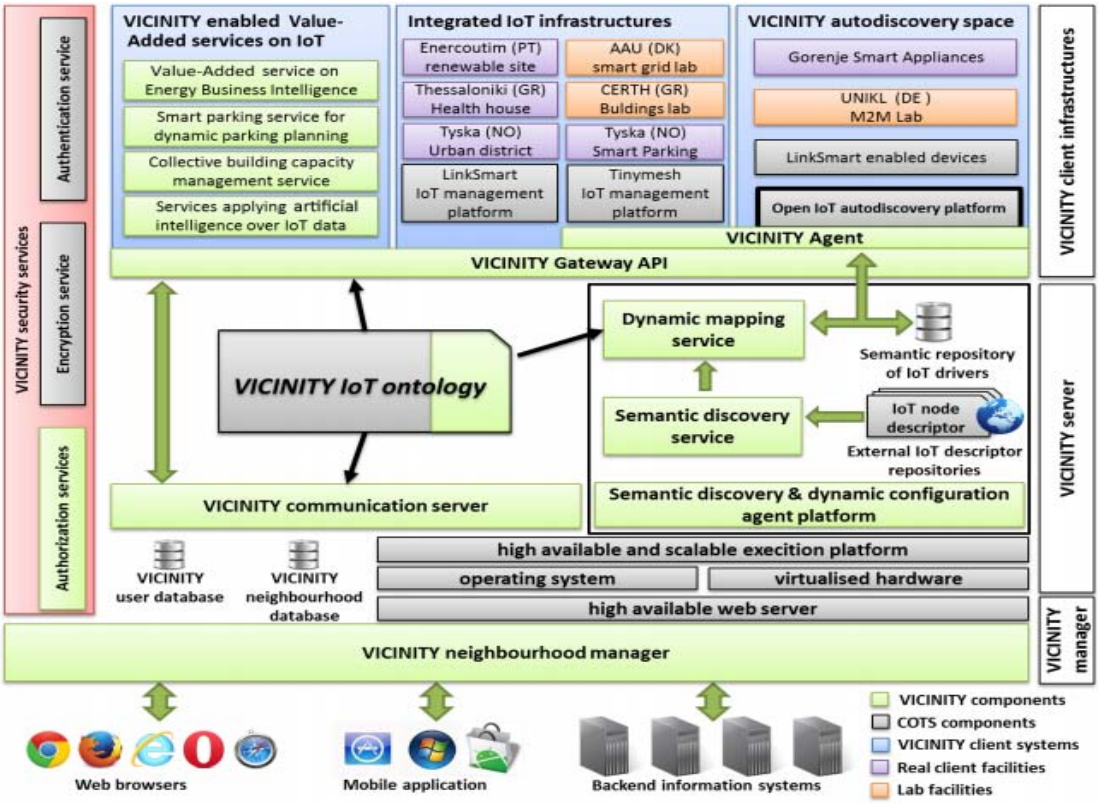

Fig. 1. VICINITY High Level Architecture

The VICINITY communication server will be responsible for communication channel setup and data forwarding according to the rules set in the VICINITY neighbourhood database, previously configured by using the VICINITY neighbourhood manager (known as the "VNM"). The communication server will use load sharing mechanisms

The VICINITY Agent can perform actions on services provided and/or events generated by the referenced IoT objects. Namely, service orchestration and choreography, as well as the filtering, transformation and aggregation of events, may be required by some consumers. Such a customized IoT object is then resolved to the low-level IoT

device and is provided by the VICINITY Agent to the VICINITY Gateway API, from where it is propagated into the guest IoT infrastructures, added value services, or end-users.

B. *Decantralization in VICINITY*

The concept of decentralization in VICINITY is expressed by the fact that the platform includes neither central operator roles nor central databases to store sensitive data about users. Instead, it connects different smart objects into a "social network" called as the "virtual neighbourhood", where infrastructure owners keep under control their shared devices and data, thanks to web-based operator console called as the VNM. Thus, each smart object owner possesses their own catalogue of shared resources and foreign resources that other users have shared with him/her. Using the VNM, the user can control which of his/her IoT assets are shared with whom and to which extent. To get connected to the VICINITY platform, the users are provided with the VICINITY open interoperability gateway. Integration to VICINITY can happen on:

- Network/infrastructure level – to connect proprietary IoT infrastructures. In that case, the users (or their system integrators) just need to take the open VICINITY gateway API with sample implementations and can easily develop an adapter to the platform. Once an IoT infrastructure is integrated to VICINITY, its owner can simply manage the access to his/her IoT data and controls using the VNM.
- On IoT device level – to connect standard IoT infrastructures. Then the task of the user is even simpler. He/she just needs to take the open VICINITY auto-discovery device and to register it with the help of the VNM. The device will automatically discover the smart objects and they will appear in the user's device catalogue on the VNM. Then, the user can manage the access rules to his/her discovered smart objects, using the VNM.

Once an IoT infrastructure is connected to the VICINITY platform, the traditional IoT value chains become unlocked. This "opens the doors" toward seamless interoperability between IoT islands present in the current IoT landscape and also enables the exploitation of independent value added services, including various cross domain IoT applications.

C. *VICINITY eHealth use cases*

VICINITY eHealth use cases are targeting typical daily environments, both indoor and outdoor, aiming to assist people while performing their daily activities and when they are old living alone; thus, the environments participating in these use cases can range from homes to public spaces (e.g. stadiums or gyms) and city centres to rural and remote areas. The diversity of these environments can showcase the VICINITY platform interoperability, since it spans over a number of various IoT installations, which are currently isolated and managed as closed systems.

The eHealth use cases are divided into two main subcategories:

- eHealth and Assisted living, *and*;
- Fitness and Preventive Medicine.

These use cases aim to demonstrate a completely new type of applications, built on top of interoperable platforms. By using sensors, actuators and integrated communication devices installed at home, in parallel with continuous remote monitoring of end-users' health parameters, VICINITY ecosystem manages to provide a direct means of communication with a 24-hours call centre with specialist staff, in case assistance is needed. This use case is considered as an important step to fulfill the need to move from institutional care to assisted living at home environment, in particular for elderly people living alone and people with long-term needs and chronic illnesses (such as people with hypertension, dementia and obesity).

Additionally, in preventive medicine, electronic medical care services enable middle-aged people to obtain a better quality and independent life by using smart wearable sensors and IoT proximity sensors to track their everyday activities and promote a healthier lifestyle. Fig.2 provides an illustration of the corresponding VICINITY use case, as developed at the municipal level of Pilea-Hortiatis in Greece, for supporting assisted living and eHealth.

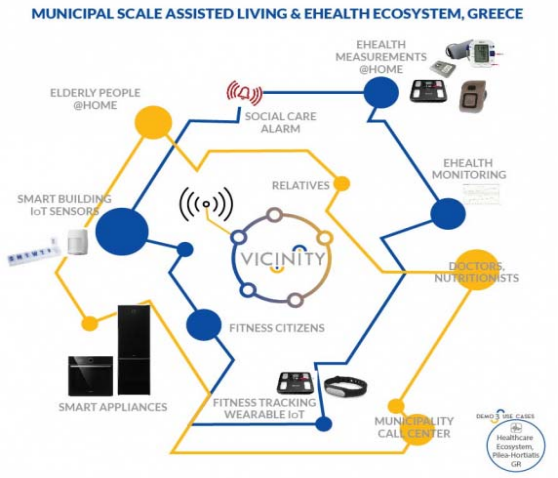

Fig. 2. VICINITY Assisted Living Ecosystem [5]

III. MAJOR CHALLENGES OF IOT SYSTEMS IN THE EHEALTH ENVIRONMENT

Many health issues, mainly in rural and remote areas, get addressed with delay due to difficulties in accessing healthcare facilities. While in severe cases a patient might lose his life, it is more often for patients to "skip" the visit to a doctor and practice medicine on their own. Thus, eHealth is an important area of concern and, along with supporting connected technologies, will play an important role in the future. To this aim, the IoT presents a huge opportunity for many "actors" in the global market and especially in the emerging market of eHealth. But as IoT systems are developed and deployed, new areas of concern and obstacles are also surfacing. Aspects such as privacy and security, vulnerability issues, ethics, health communication and enhanced transparency need to be adequately addressed, before any reliable and affective service offering.

From the healthcare providers' perspective, IoT has the potential to reduce costs, increase the quality of life and also enrich the user's experience. In addition, seamless and

secure connectivity across patients and healthcare professionals are expected to support chronic diseases, early diagnosis, real-time monitoring and medical emergencies [6]. Finally, IoT applications through their ability for dynamic changing and large scaling, may ensure the provision of high quality services within the constraints of things, such as privacy protection and semantic consistency between physical things and their associated virtual counterparts.

The following figure (i.e., Fig.3) depicts the most important trends in the eHealth domain (based on the context originally proposed in [7]). As we can easily identify, the ubiquitous and secure communications across all stakeholders is an issue of high importance.

Fig. 3. Healthcare trends and opportunities

There are three major categories of challenges in the IoT world that need to be addressed, especially when it comes to eHealth, that is: technological, business (e.g., cost analysis and new business models) and societal (e.g. new diseases and disorders)[8]. In the actual paper our work focuses upon the first category, starting from the barriers surfacing from the lack of interoperability due to vendors' restrictions.

Barriers that have been identified from the VICINITY project are:

- Lack of IoT protocol interoperability (systems are often vendor locked, by design).
- Interconnected smart objects of different owners require data sharing that raises serious privacy issues.
- IoT component vendors might be reluctant to share interface specifications (Intellectual Property problem).
- Large-scale integration imposes rules that are disadvantageous for particular participants.

In the present world wide web (www) framework -as we actually perceive it- the interoperability is one of the most important requirements for connectivity and communication among protocols and related applications. The global practice implicates that different vendors and different industries use different standards and/or interfaces to support their own applications. The interoperability to be brought by the context VICINITY will "release" the vendor locks that are present in the current IoT ecosystems and will so support the transition towards independent value added services across IoT domains, taking advantage of the availability of big amounts of data in semantic formats that are generated by IoT assets.

As far as the eHealth domain is concerned there are more issues that should be considered, namely security and privacy, which are fueled by various considerations such as lack of interoperability, geographical and administrative scattering of processes as well as security mechanisms. Additionally, low complexity at end-point platforms and lack of specified architecture along with lack of compliance with security policies, do create operating limitations [9].

IV. Security Considerations in the eHealth Domain

Protecting an IoT eHealth ecosystem is a sophisticated and demanding task since every single IoT device might present a potential risk that could be exploited to either harm the end-users or jeopardize the privacy of them [10]. Although security requirements of IoT systems and applications could be different, they all need to follow certain security policies consistent with their role and taking into account the considerations and the practical limits of the devices in question. Especially in healthcare and assisted living applications, where there are stringent privacy requirements dictated by the existing regulation, some consequently strong security mechanisms are needed. In this scope, some security requirements have been acknowledged by the ISO/IEC as part of the development of standards for the IoT [11].

Several eHealth applications in an IoT environment do run on a number of components, including sensors networking, processing and storage elements, medical devices gateways and mobile devices. The overall level of security of the system is upper-bounded by the security level of each component in the specific system, regardless its complexity. For example, for sensors which are designed to operate with computational limitations a security challenge could be the maximization of security performance at the same time the resource consumption is at its lower point. In order to tackle possible attacks, IoT devices should always verify that the received information belongs to a trusted IoT system. Under a more generalized context, security measures may include authentication, authorization management, secure booting (i.e., prevent unauthorized applications to be executed), application sandboxing, whitelisting, protection of data during capture, storage, and transit, traffic filtering features, fault tolerance, password enforcement policies, secure pairing protocols and secure transmission mechanisms (see, *for example*: [12] and [13]).

Networks participating in eHealth architectures have multiple layers of prevention, detection and response controls as the network spans through different types of networks with mixed access network protocols (such as Wi-Fi, and ZigBee). Additionally, the operating environment of each one is very important. In general, a home or a medical facility is considered as a "trusted environment", where the communication may not need to be encrypted. However, in any environment that is not considered as trusted, it is necessary for the relevant communications to be encrypted [14]. Trusted routing mechanisms, message integrity verification techniques (using hashing mechanisms such as MD5) as well as point-to-point (P2P) encryption techniques based on cryptographic algorithms are some of the methods used to secure IoT networks.

An IoT network topology is dynamically changing endlessly since new devices can enter while others might leave anytime and anyplace. This, in addition to the fact that the number of IoT devices has been increasing progressively in the recent time, constitutes a critical challenge for the security experts; especially, since the devices participating in such a network greatly vary in terms of power, computation and memory capabilities. Finally, it is of high importance that the IoT-based devices and sensors do not reveal their data to the neighboring nodes. Similarly, the tags have to be able not to transmit their data to any unauthorized reader [15]. Therefore, not only the overall system must be designed with security in mind, but also even the simplest of devices.

The volume of generated data and its management along with issues of security and privacy are a crucial aspect in the IoT context. Initially, data should always be available to the user whenever needed and all authorized parties should have ensured and immediate access to their resources under any circumstances, without disruptions and with high reliability. Furthermore, in case of sensitive information (such as health data), users should be confident that their personal data is not disclosed to any unauthorized parties. In these cases, data encryption might be used alone or in addition to two–step verification from two dependent components, or maybe biometric verification in which every user is unique.

In the VICINITY ecosystem, multiple levels of security should be addressed. Since the adapters used are proprietary (due to vendor's lock) and the devices that are running the adapter might not have enough processing power to utilize secure communication with VICINITY Open Gateway API, thus secure transfer and processing of the information up to the point of being processed by Gateway API cannot be guaranteed.

The VICINITY Security architecture relies upon standard commercial off-the-shelf solutions; however, the latter are following several key-differentiators [16]:

- Access to device data/ controls and events are defined directly by data owner in VICINITY Neighbourhood Manager through data access contracts –consents.
- Access to data defined by data owner is enforced on VICINITY Open Gateway API, preferably in data owners' infrastructure.

V. SUMMARY AND NEXT STEPS

Interoperability constitutes a significant issue to IoT systems, as existing IoT devices are highly heterogeneous in terms of underlying communication protocols, data formats and technologies. The fast emerging need for IoT applications and services "highlights" the necessity of interoperability across several IoT platforms for a unified and secure sharing. In the near future the IoT market is expected to grow but, simultaneously, the need for more and better applications that cover multiple aspects of the everyday life (such as eHealth) is not met yet.

VICINITY proposes an IoT-based ecosystem able to provide interoperability among heterogeneous IoT devices in the healthcare domain. This ecosystem has taken into consideration all security and privacy requirements referring to such a dynamic environment and, since healthcare services are highly "sensitive" requiring guarantees in terms of security, reliability, maintainability and time, stringent policies and security measures are introduced in health data communication among authorized users, organizations and applications. All the above will be evaluated and validated through field trials that will take place within the original VICINITY framework in the year to come.

ACKNOWLEDGMENT

This work is supported by the H2020 VICINITY project, which has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No.688467. The authors would like to cordially thank the entire VICINITY consortium for their valuable comments and support.

REFERENCES

[1] P.N. Howard, "How big is the Internet of Things and how big will it get?" The Brookings Institution (2015). (Retrieved on June 26, 2015).

[2] P.M. Adhao and R.B.Mapari, "The Internet of Things (IoT): New age," International Journal of Engineering Development and Research, vol. 5(2), pp. 352-357, 2017.

[3] World Wide Web Concsortium (W3C), "Semantic Sensor Network Ontology", Semantic Sensor NetworkS Incubator Group (2017). https://www.w3.org/TR/vocab-ssn/

[4] VICINITY (Open virtual neighbourhood network to connect intelligent buildings and smart objects) H2020 project, GA No.688467. https://www.vicinity2020.eu/vicinity/

[5] VICINITY Project, "Pilea-Hortiatis (GR) - eHealth and Assisted Living". https://vicinity2020.eu/vicinity/content/pilea-hortiatis-gr-%E2%80%93-ehealth-assisted-living

[6] S.M. Riazul Islam, D. Kwak, Md H. Kabir, M.D. Hossain and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," IEEE Access, vol. 3, pp. 678-708, 2015.

[7] K. Vasanth and J. Sbert, "Creating solutions for health through technology innovation – White Paper." Texas Instruments Inc. [Online]. http://www.ti.com/lit/wp/sszy006/sszy006.pdf

[8] K. Narayanan, "Addressing The Challenges Facing IoT Adoption." Keysight Technologies, Santa Rosa, California (2017)

[9] D. Minoli, K. Sohraby and B. Occhiogrosso, "IoT Security (IoTSec) Mechanisms For e-Health and Ambient Assisted Living Applications." In Proccedings of the IEEE/ACM 2017 International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE'17). IEEE/ACM, 13-18, 2017.

[10] G. Suciu, V. Suciu, A. Martian, R. Craciunescu, A. Vulpe, I. Marcu, S. Halunga and O. Fratu, "Big data, internet of things and cloud convergence – An architecture for secure e-health applications," Journal of Medical Systems, vol.39(11), p.141-148, 2015.

[11] International Organization for Standardization / International Electrotechnical Commission (ISO/IEC), "Study Report on IoT Reference Architectures/Frameworks". ISO/IEC, 2014.

[12] Symantec Corporation, "Internet of Things (IoT) Security." https://www.symantec.com/products/internet-of-things

[13] https://www.windriver.com/iiot/

[14] D. Lake, R. Milito, M. Morrow and R. Vargheese "Internet of Things: Architectural Framework for eHealth security," Journal of ICT, Vol. 3&4, pp. 301–328, 2013.

[15] D. Miorandi, S. Sicari, F. De Pellegrini and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks ,vol. 10(7), pp.1497-1516, 2012

[16] VICINITY Project, "Deliverable 4.3: VICINITY Security Services". https://www.vicinity2020.eu/vicinity/content/d43-vicinity-security-services