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

Secure IoT e-Health Applications using VICINITY Framework and GDPR guidelines

Maria Koutli*, Natalia Theologou*, Athanasios Tryferidis*, Dimitrios Tzovaras*, Aimilia Kagkini†, Dimitrios Zandes†, Konstantinos Karkaletsis†, Konstantinos Kaggelides†, Jorge Almela Miralles‡, Viktor Oravec‡, Stefan Vanya‡

* CERTH/ITI - Centre for Research and Technology Hellas/Information Technologies Institute, 6th km Harilaou - Thermi, 570 01, Thessaloniki, Greece

† Gnomon Informatics, 21 Tritsi Street, 570 01, Thessaloniki, Greece

‡bAvenir, s.r.o., Kladnianska 34 821 05, Bratislava, Slovakia

Email: {mkoutli, nataliath, thanasic, dimitrios.tzovaras}@iti.gr, {a.kagini, d.zandes, k.karkaletsis, k.kaggelides}@gnomon.com.gr, {jorge.almela, viktor.oravec, stefan.vanya}@bavenir.eu

***Abstract*—In this work we analyze the security requirements and challenges of e-Health Internet of Things (IoT) applications and propose a complete architecture to address them. This architecture combines VICINITY IoT Framework security features together with General Data Protection Regulation (GDPR) compliant mechanisms in order to provide secure e-Health services to elders and middle-aged people. We also demonstrate how an Ambient Assisted Living (AAL) and an mHealth application were designed and implemented, addressing the current security and privacy requirements.**

***Index Terms*—IoT, security, e-Health, privacy, GDPR**

I. Introduction

IoT e-Health applications are increasing in recent years. Healthcare applications are moving from hospital centered applications towards patient-centered applications [1]. Security and privacy are major concerns for the use and acceptance of IoT in health domain. The use of VICINITY Platform combined with secure storage and authorized data transactions respecting GDPR regulations, aims to address security challenges of e-Health IoT applications.

This paper is organized as follows; section II presents an overview of the security requirements and challenges in the e-Health IoT domain. Section III provides a detailed report of the related work that has been conducted regarding security in IoT systems. Security features of the proposed VICINITY IoT platform and data privacy mechanisms are presented in sections IV and V respectively. Section VI illustrates the proposed architecture that is used for addressing security challenges in e-Health domain and the paper concludes in section VII.

II. Security Requirements and Challenges

IoT sensors and devices provide an internet connection to the physical world, giving the ability to sense it and make control actions. This aspect, increases the already well-known security risks of internet applications in the areas of communication, access control and data manipulation. A recent survey on the security of well-known, commercial IoT frameworks [2], such as AWS IoT, SmartThings, Azure IoT, has showed that they are considered robust as long as they provide security features, such as authentication, authorization, encryption etc. On the other hand, they all have a cloud based architecture with centralization of data, which arises many privacy concerns.

The IoT architecture is divided into three different layers namely, Perception Layer (or Sensor Layer), Network Layer (or Transmission Layer) and Application Layer (or Business Layer), each one requiring different security mechanisms [3]. Several recent studies on the field of IoT security [3], [4], [5], [6], [7] have suggested that the main security features of IoT applications are the following:

- Authentication (Application/Network Layer): It is the process that is used to verify the identity of the devices or users in the network. Even though authentication was considered the most popular research subject for IoT security during 2016–2018 [6], it still has weaknesses. IoT due to its constrained nature, requires a lightweight on the one hand but trustworthy and robust on the other hand authentication scheme.
- Authorization (Application/Network Layer): Authorization, concerns the rules regarding what the users or devices can access after their identity has been verified. Authorization rules are used to guarantee data privacy which is an important security principle since many devices, services, and people are sharing the same communication network in IoT [8].
- Confidentiality, Encryption (Application/Network/Physical Layer): An encryption mechanism for data transmission over the internet is required in order to ensure the confidentiality of data. Due to memory and CPU constraints the encryption algorithm needs to be efficient.
- Integrity (Application/Network Layer): Data integrity means to ensure that data are received from the correct

2325-2944/19/$31.00 ©2019 IEEE
DOI 10.1109/DCOSS.2019.00064

source without any corruption.

- Availability (Application Layer): Availability is to ensure that the data can be reached by authorized users whenever they are requested.
- Privacy (Application/Network Layer): Privacy concerns the protection of data from unauthorized access. Authorization and anonymization techniques are usually used towards this direction.
- Trust management (Network Layer): Allows IoT nodes to evaluate the trustworthiness of one another, which helps to identify malicious nodes in the network.

Addressing the above security features is required for considering an IoT application secure. Apart from the general IoT security requirements, health IoT applications have to deal with further ethical and privacy concerns. The vast amount of sensitive personal data that is collected, includes information concerning movement, location, activities and health measurements of people. This, makes security in health applications even more demanding, since they have a major impact in many aspects of the every day life.

The consent of the IoT devices user to the requester of his/her personal data is required in order to address the risk of data collection through IoT devices without the user being aware of it. O'Connor et al. argue in [9] that the first step for global acceptance and usage of health IoT applications, is to ensure that the IoT users are fully aware to whom and for which data, they give consent to, when they participate in IoT e-Health programs. The European Union's (EU) General Data Protection Regulation (GDPR), which has gone into effect in May 25, 2018, helps towards this direction. The regulation sets rules for protection of personal data of citizens in transactions within the EU. The following guidelines are important for creating IoT Health applications that respect GDPR:

- Consent: The request for consent must be provided in an easily accessible form, with the data processing purposes attached to that consent. It must be as easy to withdraw the consent as it is to give it.
- Privacy by Design: Privacy by design concept has existed for many years, but with GDPR it is becoming part of a legal requirement. The work of Perera et al. [10] proposes a privacy by design framework with 30 guidelines. These guidelines can be further grouped in:
  - Data minimization, refers to the processing of only the absolutely necessary data. This includes minimization of data sources, raw data, data storage etc.
  - Data anonymization and encryption for communications, processing and storage
  - Avoid dissemination of raw data and reduce data granularity
  - Distributed data processing and storage
  - Data aggregation
  - Logging and auditing of data transactions
  - Open source
  - Standardisation
  - Compliance to laws and policies
- Right to be Forgotten: It is also known as Data Erasure, and refers to the right to erase the subject's personal data, and potentially have third parties halt processing of the data.

This paper proposes an architecture that aims to address the major security requirements of the IoT Application Layer, and to respect the ethical and privacy regulations for data protection in e-Health applications that were mentioned above.

III. RELATED WORK

The vast growth of IoT technology, due to the increase in the integration of devices in IoT and issues in reliability, has aroused many subjects regarding security in all three different layers of IoT. In the Perception Layer of the overall architecture, devices depending on their size are secured through different algorithms executed on constrained environment as proposed in [3].

Devices and services are vulnerable to Denial of Service attacks (DoS) and security must be addressed as in [11] where Kim, Holz, Hu and Jha represented cryptographic DoS attacks in models using different protocols concluding in their vulnerability. They proposed a server puzzle construction for the vast majority of protocols. End-To-End security communication between devices and application is a challenging issue especcially in e-Health domain. Choi et al. in [12] have proposed an IoT framework which encrypts sensitive data using CP-ABE and AES while the decryption occurs only if a sequence of attributes are satisfied.

In e-Health applications strong security mechanisms are demanded due to strict privacy requirements. In many cases authentication and authorisation methods are implemented for ensuring security as in [13] where Moosavi et al. use a certificate-based Datagram Transport Layer Security (DTLS) handshake protocol between end-user and smart e-health gateway due to the difficulty in implementing cryptography techniques in resource constrained sensors.

In VICINITY Case we examine the security issues regarding the sharing access rules between devices, services and devices owners. Various architectures have been proposed for this kind of authentication like in [14] where Sridhar and Smys use unique Device ID of the sensors to authenticate devices and services through generating key pair. This way fault packages and illegitimate attacks are eliminated. In a similar context Kim, Jeon and Kim in [15] have implemented a registration process including device authorization in the security framework by creating device token. Authentication protocol for embedded devices and cloud servers is described in [16] based in ECC expoliting its efficient computation and small key sizes using HTTP cookies stored on the device. Similar to VICINITY, Porambage et al. in [17] have conducted a two-phase authentication protocol for Wireless Sensor Networks (WSN) in order to implement authentication between sensor nodes and end-users. Phases include obtaining cryptographic credentials and authentication. However, the paper does not cover authorization for access control whereas VICINITY

covers this issue by conducting contracts between the devices and the applications.

Finally, blockchain is commonly exploited for solving security issues in communication layers between devices, gateways and cloud due to decentralization, privacy by design principle, transparency and autonomous interaction as depicted in [18]. In the same paper, Ouaddah proposed FairAccess and PPDAC, lightweight access control frameworks for constrained devices with the intention to solve traceability and profiling as well as storing in blockchain, which represents a database, all access control policies in form of transactions offering auditing functions.

IV. THE VICINITY FRAMEWORK SECURITY FEATURES

A. Description of the Platform

VICINITY is an IoT framework and platform that aims to provide semantic interoperability between different IoT platforms and vendors [19]. VICINITY also tackles the issues of IoT security and privacy in order to offer a complete and robust solution. The framework proposes a decentralized architecture consisted of nodes, which communicate through secure peer-to-peer (P2P) network, under authorization principals. The VICINITY architecture is presented in Fig. 1. As it can be seen, the user data communication (in red) is node to node communication, without the platform storing or being aware of the exchanged data. Only semantic metadata information is communicated to the platform (in yellow and blue).

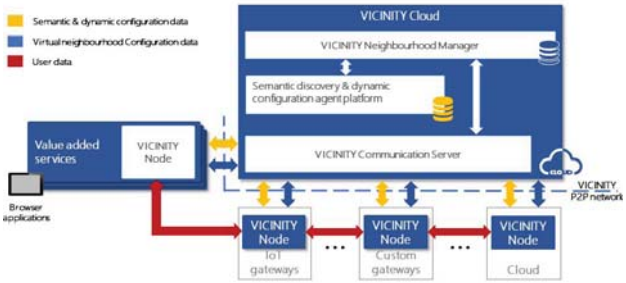

Fig. 1. The Vicinity Platform Architecture.

Before we continue with the description of the framework, we need to refer to the entities which are defined in VICINITY:

1) User: A user is a physical entity, that can have different roles or authorization levels, and it is a member of an Organization. Users can set their visibility within the platform in order to keep their privacy.
2) Organization: It can be any company or association that owns IoT devices or services. Many Users can belong to one Organization.
3) Thing (or Item): A Thing can be either a physical entity as a smart device, sensor or a service. Things are registered in VICINITY under a specific User, Organization and Access Point. Things are also linked to a visibility or privacy rule.
4) Access Point: It is the virtual representation of an IoT infrastructure.
5) Friendship: It is a privacy agreement between two Organizations, regarding the visibility of their Users and Things.
6) Contract: It is a privacy agreement between one or more devices/services and a service, regarding data access and control.

VICINITY platform provides a cloud infrastructure, which is responsible for the registration and handling of the aforementioned entities. VICINITY Cloud is composed by three main components:

- Neighbourhood Manager: It provides all the functionality for User, Organization registration, creation of Access Points, Friendships and Contracts and handling of visibility rights. It is composed by a dedicated API and a web interface.
- Semantic Repository: It stores all registered Things in VICINITY and their metadata information, such as the name, owner, location etc.
- Communication server: It is used to setup communication channels between VICINITY Nodes and control exchange of user data.

VICINITY Nodes are composed also by three components:

- Gateway API: Provides HTTP REST services locally close to the connected infrastructure. It is responsible for the P2P communication between different Things (VICINITY Nodes), respecting the Contracts that have been set in Neighbourhood Manager.
- Agent: It is responsible for the bottom-up registration and updates of Things in Semantic Repository and provides common functionality, as for example subscription to events.
- Adapter: Provides a simple API for the translation of the local IoT infrastructure in VICINITY terms; it also provides, a formal description of the registered Things and the associated VICINITY compliant endpoints it exposes to VICINITY.

B. Privacy features

VICINITY allows Users, that have an appropriate role, to register their IoT devices and services (Things), discover other registered Things and allow their Things to be discovered, according to the privacy rules they have set. This is a privacy feature of the Platform beyond the scope of machine-to-machine (M2M) communication, which is offered by Neighbourhood Manager component.

VICINITY has privacy rules both regarding ”who can see what” and also regarding ”who can access what”. Regarding the first category, a VICINITY User can have different roles, each of them giving the ability to perform certain actions:

- Device owner: can perform actions related to devices.
- Service provider: can perform actions related to services.

- Infrastructure operator: is able to manage Contracts
- Administrator: it is the user that registers an organization who gets this role by default. Administrator can modify the Organization's properties, remove an Organization and update Users roles.
- System integrator: is able to create and manage Access Points.
- User: can view the items of the Organization and make very limited actions

Moreover, Users can set their privacy level, which can be:

1) Private
2) Visible to Friends or
3) Public

Users can also set the privacy level of each Thing that they have registered in VICINITY, according to their role. The privacy levels range from:

1) Private: Visible only within the User's Organization.
2) Visible to Friends: Visible to all befriended Organizations.
3) Public: Visible for all Organizations.

Regarding the second category, "who can access what", VICINITY Neighbourhood Manager allows an IoT Operator to request a service for one, many or all of his/her devices/services. If the service provider accepts this request, then a Contract is created. This means that the service can access (or control depending on the contract rules) any of the contracted devices and services. This functionality is actually offered through the Gateway APIs of each VICINITY Node in cooperation with the Communication Server. A Contract can be taken back at any time preventing any previous communication.

C. Security features

VICINITY Framework provides security through authentication, authorization and encryption mechanisms. Neighbourhood Manager provides secure communications by:

- User authentication
- Authorization rules (mentioned above)
- Storing hashed passwords
- SSL communication

Moreover, VICINITY provides secure communication of devices and services based on the open messaging standard RFC 6120 [20], known as XMPP. Communication between VICINITY Nodes that are behind a NAT or not included in public IP addressing scheme is performed by Gateway API with:

- Things' authentication: Things log in the XMPP network via Gateway API and Agent, with their credentials, which were automatically created after their registration. Credentials are managed by the Agent, which is the responsible component for Things registration.
- End-to-end encryption: Encryption of the messages before their transmission over the XMPP network is performed. In order to encrypt the communication channel between two VICINITY Nodes, STARTTLS with TLS 1.2 encryption scheme is used.
- Thing's authorization: In cooperation with VICINITY Communication Server, the Gateway APIs allow or deny communication between two Things, according to Contracts.

While VICINITY, manages to address most of the current security challenges in IoT, yet there are privacy concerns beyond the general IoT scope which are related to specific e-Health IoT applications. In the following section we will present the mechanisms that we chose for dealing with privacy in two e-Health applications, complementary to the use of VICINITY IoT platform.

V. Data storage and processing

E-Health applications usually consider the following user roles: the patient, which could be an elder living alone or any person in need of medical supervision, the health professional, which could be a doctor, dietitian or psychologist and the guardian, which could be a relative, neighbour or a caregiver. Some of the questions that arise in this case are: "who can access the patient's medical data?", "which of the data are available and in what format?", "is the patient aware of the purposes of the use of his/her data?". In our e-Health applications we aim to answer these questions by providing a secure mechanism for storage and processing of the medical data, which requires the patient's consent for data sharing.

Using VICINITY, a decentralized IoT platform, allows e-Health applications architecture designers to be in charge of the privacy of the patients' data and not depend on a third-party storage of a centralized or cloud-based IoT platform. Since VICINITY platform does not store any data coming from the IoT devices it does not offer any privacy mechanisms for IoT data storage. Nonetheless, VICINITY respects GDPR regarding the storage of devices and services metadata and users information.

Our e-Health solution that extends our work in [21], includes a service that is responsible for the storage of sensitive personal data in order to be available for further processing. The storage service, respecting the GDPR, gathers the data coming from the patients' devices and sensors and supports the following functionality:

- Handling of consent for data access
- Auditing of data transactions
- The right to be forgotten

The offered medical services of our solution, include individual medical data processing, abnormal detection, gamification and aggregated data processing services. The aforementioned services do not have a direct access to the medical devices and sensors but they fetch the raw data from the storage service instead, in order to audit all the data transactions. The architecture of our solution is presented in Fig.2. The doctor and the guardian of the patient can access both raw and analyzed data, after they have received consent from the patient. Moreover, the patient is entitled to request at any time

who has accessed his/her measurements and to retrieve back the consent he/she has given.

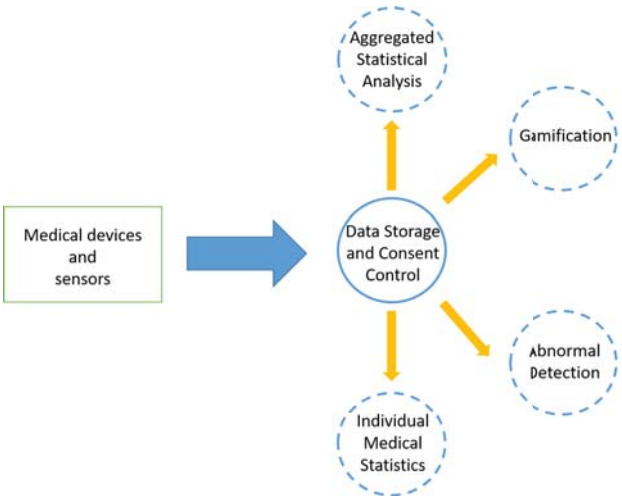

Fig. 2. Data Flows.

VI. PROPOSED ARCHITECTURE FOR E-HEALTH APPLICATIONS

A. Ambient Assisted Living (AAL) Application

The ageing of the world population and the emerging usage of IoT, has promoted the study of IoT systems and architectures for ambient assisted living (AAL). AAL aims to increase the quality of life of elder people or disabled by providing a secure and protected living environment [22]. This application demonstrates how sensors and medical devices deployed in different homes, securely communicate with services for data analysis, in order to provide assisted living operations to elders who live alone. In cooperation with the local municipality of Pilea-Hortiatis healthcare assistants, a number of elder people have been targeted and offered this application. The demonstration of this use case is important in terms of security, because it involves real and sensitive data from different homes, which have to be handled with great caution.

1) Hardware of the application: Elderly citizens homes have been deployed with building sensors and medical devices in order to remotely monitor their routine tasks, everyday activities and medical data. In this application we have defined two types of elderly citizens homes, according to the deployed equipment:

House Type 1

- Medical devices
  - blood pressure monitor devices
  - weight scales
  - panic buttons

House Type 2

- Occupancy sensors
  - door sensors
  - motion detectors
  - bed pressure sensors
- Smart appliances
  - fridge
  - oven

A Raspberry Pi is used as a gateway that collects the sensor data and forwards them to the Storage service through internet connection using VICINITY P2P network.

2) Offered services: Individual medical statistics service is offered to elders of House Type 1, while Monitoring and Abnormal Behavior Detection service is offered to elders of House Type 2.

Individual medical statistics service collects medical data of elderly people living alone allowing health care providers and relatives to know their current condition in order to provide advises and check whether there is aberration. Blood pressure monitor, weight and panic button measurements of elders are processed in order to classify an elder according to the frequency of taking measurements (frequent, normal, sparse) and the usual time he/she takes measurements. Moreover, minimum and maximum measurements' values are presented, while notifications are also produced in cases that a measurement exceeds specified limits e.g. for high blood-pressure. Notifications are also produced in cases that the elder forgets to take measurements regularly.

In the case of Monitoring and Abnormal Behavior Detection service, the building sensors and smart appliances' data are collected in real time and allow tracking of elders' activity at home. The data are analyzed in order to produce behavior metrics such as movement per hour, mobility between rooms, duration in rooms, appliances usage and others. Behavior metrics are then used in order to create normal behavior models and thus, be able to detect future abnormal conditions and raise events. The normal conditions are determined per person, according to his/her usual habits, which are extracted from the monitored building sensor data.

3) Architecture: In this e-Health application, elders' sensor data are transferred securely through the VICINITY IoT platform to the service that is responsible for data storage and consent control. The AAL services process the raw data and convert it to valuable information to the people who monitor the elder. In this scenario, we have three user roles - reflecting to Organizations in terms of VICINITY, the elder, the health-professional and the guardian. Each elder's home is an Organization with a small IoT infrastructure of sensors. The provider of the services is also an Organization in VICINITY.

The Friendships between the VICINITY Organizations are the following:

- Elder Homes with Service Provider
- Doctors with Service Provider
- Guardians with Service Provider

and the contracts between the VICINITY Things are:

- Each Elder's sensor (medical or building) with the Storage and Consent Control service

- Each Doctor application with the Storage and Consent Control, Individual Statistics and Abnormal Detection services
- Each Guardian application with the Storage and Consent Control, Individual Statistics and Abnormal Detection services
- Individual Statistics and Abnormal Detection services have by default a contract with the Storage and Consent Control service since they are registered under the same Organization

Each elder has to specify a Doctor and a Guardian to whom they give consent to access their data. While the Elder's sensors forward the measurements to the Storage and Consent Control service and the Doctors and Guardians can request data from the same service, "who can access which data" is handled by the consent concept. For example Elder1 has given consent to Doctor1 and Guardian1 who can access the Elder1 raw and processed data, while Doctor2 cannot.

In every communication request between two VICINITY Things, the VICINITY Gateway communicates with VICINITY Communication Server in order to determine whether the Things can see each other and allow or deny the communication. The VICINITY Communication Server sets up the visibility based on the existing Contracts in the VICINITY Neighbourhood Manager. While communication requests are handled by VICINITY privacy rules, the response of the requests is handled by the consent rules. The architecture and data flows within VICINITY can be seen in Fig.3.

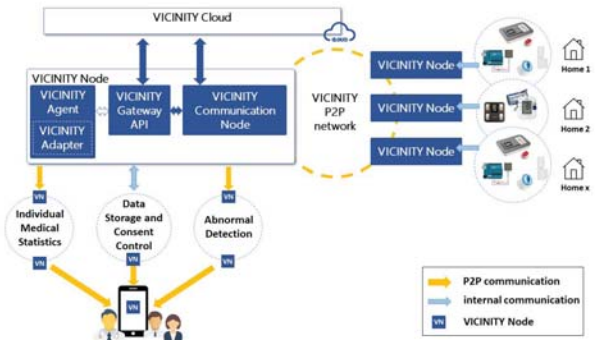

Fig. 3. The AAL e-Health application architecture.

B. mHealth Application

This application focuses on the promotion of a healthy lifestyle to middle-aged citizens of municipality of Pilea-Hortiatis. Its goal is to help the citizens to adopt new healthy habits and thus preventing, as much as possible, future health issues, meaning less visits to health care providers or dietitians and less primary institutional costs for health services.

Citizens take part in a municipal-scale competition (urban marathon) and compete with other citizens on health improvement achievements. These means will be used in order to motivate citizens to participate even more to this health improvement case study. Specialized medical staff monitor the middle-aged citizens weight measurements as well as their fitness data on daily basis and examine their improvement. Verifying the security of data from the devices extracting these information is of high importance for the case study.

1) Hardware of the application: In order to achieve mHealth application's goals the middle-aged citizens of this use case have been provided with:

- Medical devices
  - wearable fitness trackers
  - weight scales

  while,
- Beacons, small Bluetooth radio transmitters, have been deployed in the sport centres of the municipality.

Middle-aged people, can use their mobile phone as a gateway to connect via Bluetooth to the medical devices and sensors, which in turn forwards their data to the respected Storage service through internet connection using VICINITY P2P network.

2) Offered services: Urban Marathon application is based on gamification system where middle-aged citizens of municipality are categorized depending on their body mass index (BMI) and consequently distinct rules and actions applies to them. Health experts have defined number of steps, weight loss and visits to gym each user should achieve to adopt a generally healthier behavior while competing with other users. Citizens gain points when achieving the goals that the health experts propose to them and compete with other citizens. Pointing system applies different rules and awards so that anyone participating has the capability of winning the competition while continue to be competitive.

Citizens are informed for the status of their activities by using a mobile application while watching their overall progress and ranking. The mobile application is also used in order to sign up for this urban marathon and health experts are utilizing it for tracking citizens' progress.

Citizens data are gathered anonymously while statistically analyzed and dispatched to municipalities through a web application in order to be aware of citizens health status and to detect how the Urban Marathon facilitates health status and improvement of middle-aged people.

3) Architecture: The architecture of mHealth application is presented below:

Doctor, Municipality and Citizens represent organizations in VICINITY Platform. Friendships are conducted through VICINITY between:

- Doctor-Municipality
- Citizen-Municipality

Privacy agreements are implemented between services and devices of the mHealth application in order to justify secure and authorized communications between the entities involved in the case study. Therefore contracts are conducted between:

- Doctor Application-Storage and Consent Control Service: in order for doctor's application to have access to individuals' medical processed data through the application

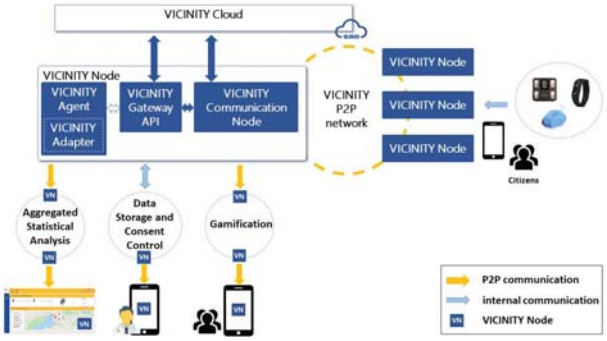

Fig. 4. The mHealth application architecture.

- Citizen Application-Gamification service: in order for citizens to track their ranking in the Urban Marathon and treatment plan created for them through the application
- Activity tracker-Storage and Consent Control Service: in order for citizens to track their daily steps through the application
- Weight Scale-Storage and Consent Control Service: in order for citizens to track their weight through the application
- Beacon-Storage and Consent Control Service: in order for citizens to track their visits to gym through the application

As shown in Fig.4 applications and devices represent VICINITY Nodes communicating with other VICINITY Nodes for ensuring authorized access and detect unauthorized one. Data are transferred through VICINITY P2P Network while access rules are defined in VICINITY Cloud.

As mentioned in section V in order to protect private medical data of individuals from unauthorised access, consent is given from the citizens to specific doctors for a specific time period, through the mobile application. The dietitian accepts the consent and creates a treatment plan for each citizen. This procedure is available by the electronic consent (eConsent) feature of the citizen and doctor mobile applications and can be withdrawn at anytime by the citizen.

C. Security in e-Health Applications

The presented e-Health applications aim to address the security and privacy requirements mentioned in section II. Table I presents a summary of the features and how they were addressed by our solution.

Table II summarizes the basic GDPR features with the respective guidelines and how they were addressed by our solution.

VII. CONCLUSIONS AND FUTURE WORK

In this paper we presented how the two e-Health applications (Ambient Assisted Living (AAL) and mHealth) cover security and privacy challenges in IoT with their integration to VICINITY platform. VICINITY components provide functionality such as authentication, authorization and end-to-end encryption. Due to the implication with sensitive and private data we further developed mechanisms for dealing with GDPR requirements in the context of consent, auditing and the right to be forgotten. The e-Health services that were implemented for processing personal medical data are accessing them through the storage service, respecting GDPR requirements.

Further implementation regarding security and privacy features, could be towards data integrity and availability, features that are not covered by VICINITY Platform. In terms of Privacy by Design guidelines, future work could include data minimization and anonymization. Moreover, we see challenges in the blockchain technology, which supports decentralized trust, and could be potentially exploited to support identity management in IoT systems rather than a centralized certificate authority [23].

TABLE I
IoT Security and privacy features

Feature	Supported	Functionality
Authentication	✓	Authentication of VICINITY devices and services / Authentication of e-Health application users
Authorization	✓	Friendships, Contracts (VICINITY) / eConsent forms for application users
Confidentiality, Encryption	✓	End-to end encryption for VICINITY communications
Integrity	–	No specific implementation
Availability	–	No specific implementation
Privacy	✓	Anonymized processing of data by the services and auditing of transactions

TABLE II
GDPR features and guidelines

Feature	Guideline	Functionality
Consent	Request Consent	✓eConsent
Privacy By Design	Data minimization	–
	Data anonymization	–
	Data granularity reduction	✓for Behavior Monitoring
	Distributed data processing and storage	✓data not stored by VICINITY Platform
	Data Aggregation	✓
	Logging and Auditing	✓
	Open Source	✓VICINITY Platform
	Standardisation	✓based on XMPP (RFC6120)
	Compliance to laws and policies	✓GDPR
Right to be Forgotten	Data Erasure	✓

Acknowledgment

This work is supported by the H2020 VICINITY project, which has received funding from the European Unions Horizon 2020 research and innovation programme under grant agreement No 688467. The authors would like to thank the entire VICINITY consortium for their valuable comments and support. This paper reflects only the authors views and the Commission is not liable for any use that may be made of the information contained therein.

REFERENCES

[1] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, "Towards fog-driven iot ehealth: Promises and challenges of iot in medicine and healthcare," *Future Generation Computer Systems*, vol. 78, pp. 659–676, 2018.

[2] 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.

[3] N. Khan, N. Sakib, I. Jerin, S. Quader, and A. Chakrabarty, "Performance analysis of security algorithms for iot devices," in *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, Dec 2017, pp. 130–133.

[4] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of things security and forensics: Challenges and opportunities," *Future Generation Computer Systems*, vol. 78, pp. 544–546, 2018.

[5] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[6] W. H. Hassan *et al.*, "Current research on internet of things (iot) security: A survey," *Computer Networks*, vol. 148, pp. 283–294, 2019.

[7] G. K. Saha and S. Kumar, "Security issues in iot-based healthcare," *International Journal of Applied Research on Information Technology and Computing*, vol. 8, no. 3, pp. 385–389, 2017.

[8] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, Oct 2017.

[9] Y. OConnor, W. Rowan, L. Lynch, and C. Heavin, "Privacy by design: informed consent and internet of things for smart health," *Procedia computer science*, vol. 113, pp. 653–658, 2017.

[10] C. Perera, C. McCormick, A. K. Bandara, B. A. Price, and B. Nuseibeh, "Privacy-by-design framework for assessing internet of things applications and platforms," in *Proceedings of the 6th International Conference on the Internet of Things*. ACM, 2016, pp. 83–92.

[11] J. Y. Kim, R. Holz, W. Hu, and S. Jha, "Automated analysis of secure internet of things protocols," in *Proceedings of the 33rd Annual Computer Security Applications Conference*. ACM, 2017, pp. 238–249.

[12] J. Choi, Y. In, C. Park, S. Seok, H. Seo, and H. Kim, "Secure iot framework and 2d architecture for end-to-end security," *The Journal of Supercomputing*, vol. 74, no. 8, pp. 3521–3535, Aug 2018. [Online]. Available: https://doi.org/10.1007/s11227-016-1684-0

[13] S. R. Moosavi, T. N. Gia, A.-M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, and H. Tenhunen, "Sea: A secure and efficient authentication and authorization architecture for iot-based healthcare using smart gateways," *Procedia Computer Science*, vol. 52, pp. 452 – 459, 2015, the 6th International Conference on Ambient Systems, Networks and Technologies (ANT-2015), the 5th International Conference on Sustainable Energy Information Technology (SEIT-2015). [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050915008133

[14] S. Sridhar and S. Smys, "Intelligent security framework for iot devices cryptography based end-to-end security architecture," in *2017 International Conference on Inventive Systems and Control (ICISC)*, Jan 2017, pp. 1–5.

[15] J. Kim, Y. Jeon, and H. Kim, "The intelligent iot common service platform architecture and service implementation," *The Journal of Supercomputing*, vol. 74, no. 9, pp. 4242–4260, Sep 2018. [Online]. Available: https://doi.org/10.1007/s11227-016-1845-1

[16] S. Kalra and S. K. Sood, "Secure authentication scheme for iot and cloud servers," *Pervasive and Mobile Computing*, vol. 24, pp. 210 – 223, 2015, special Issue on Secure Ubiquitous Computing. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1574119215001510

[17] P. Porambage, C. Schmitt, P. Kumar, A. V. Gurtov, and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed iot applications," *2014 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 2728–2733, 2014.

[18] A. Ouaddah, "A blockchain based access control framework for the security and privacy of iot with strong anonymity unlinkability and intractability guarantees," ser. Advances in Computers. Elsevier, 2018.

[19] Y. Guan, J. C. Vasquez, J. M. Guerrero, N. Samovich, S. Vanya, V. Oravec, R. Garca-Castro, F. Serena, M. Poveda-Villaln, C. Radojicic, C. Heinz, C. Grimm, A. Tryferidis, D. Tzovaras, K. Dickerson, M. Paralic, M. Skokan, and T. Sabol, "An open virtual neighbourhood network to connect iot infrastructures and smart objects vicinity: Iot enables interoperability as a service," in *2017 Global Internet of Things Summit (GIoTS)*, June 2017, pp. 1–6.

[20] P. Saint-Andre, "Extensible messaging and presence protocol (xmpp): Core," Tech. Rep., 2011.

[21] M. Belesioti, I. P. Chochliouros, S. Vanya, V. Oravec, N. Theologou, M. Koutli, A. Tryferidis, and D. Tzovaras, "e-health services in the context of iot: The case of the vicinity project," in *Artificial Intelligence Applications and Innovations*, L. Iliadis, I. Maglogiannis, and V. Plagianakos, Eds. Cham: Springer International Publishing, 2018, pp. 62–69.

[22] D. Bacciu, P. Barsocchi, S. Chessa, C. Gallicchio, and A. Micheli, "An experimental characterization of reservoir computing in ambient assisted living applications," *Neural Computing and Applications*, vol. 24, no. 6, pp. 1451–1464, 2014.

[23] E. Bertino, K.-K. R. Choo, D. Georgakopolous, and S. Nepal, "Internet of things (iot): Smart and secure service delivery," *ACM Transactions on Internet Technology (TOIT)*, vol. 16, no. 4, p. 22, 2016.