Context-aware pseudonymization and authorization model for IoT-based smart hospitals

Salah Zemmoudj, Nabila Bermad, Mawloud Omar

Noname manuscript No.
(will be inserted by the editor)

Context-aware pseudonymization and authorization model for IoT-based smart hospitals

Salah Zemmoudj · Nabila Bermad · Mawloud Omar

Received: ../../..

Abstract Smart hospital is a healthcare infrastructure that uses IoT technology. This intelligent space allows to collaborate a several health actors via their IoT devices. This coordination improves the quality and continuity of health services for better patient care. However, uncontrolled access to patient information can disrupt the smooth running of hospital services. In this paper, we aim to secure the information of patient exchanged and shared, using the privacy and access control based on the context. We develop two protocols, the first is a context-aware pseudonym service. It protects the patient's personal and health information in two smart space hospital and home. Furthermore, we prevent the disclosure of the patient's location during his hospital stay. The second is an authorization and delegation protocol based on trust, context and role. It oversees the actions and interactions of health body with the smart bracelet object of patient. Our protocol uses the context to generate a set of roles with their trust values. Only one role is activated if its trust value is greater than or equal to a trust threshold. A dynamic delegation mechanism is created to better manage the interactions between health bodies. We demonstrate through the practical analysis as well as generation time overhead, storage overhead and response time requirement the efficiency and robustness of our proposed protocols.

Keywords Smart Hospital · IoT · Context-aware · Privacy · Pseudonym · Access Control · Authorization

Salah Zemmoudj
Tel.: +213-67-0183925
E-mail: salah.zemmoudj@univ-bejaia.dz

Nabila Bermad
Tel.: +213-66-5596028
E-mail: nabila.bermad@univ-bejaia.dz

Mawloud Omar
Tel.: +213-55-5150466
E-mail: mawloud.omar@univ-bejaia.dz

Unité de Recherche LaMOS, Faculté des Sciences Exactes, Université de Bejaia, Algérie.

1 Introduction

Traditional hospital is an infrastructure connected locally via the intranet of the hospital, the data of patient are stored as a set of records in a database, which is accessible from the local network of hospital. The authorized doctor is the only healthcare provider who can access to secret documents of the patient. Access to various data of the patient depends on the type of information stored locally in hospital, the level of privacy that has been assigned to each type of information, the role, the status of health care and the nature of the therapeutic relation. However, there are doctors, nurses and other hospital staff (administrator, agent, director, etc.) who can access to medical record without the authorization of patient for various reasons, including the alteration of the patient's personal and health information, the steal of patient's private information, and the throwing of a patient's medical record.

The increasing number of wireless medical devices creates the vision of the connected hospital. The connection of these devices may improve the quality of patient care, the management information (treatment, manipulation, and updated), the availability of electronic health record (EHR) and the information that it contains. In the connected hospital, the flow of patient's data is done locally via an intranet local network, or between health care establishments via Internet. Doctors, nurses, visitors, other patients and hospital staff can access to various databases of establishment to change, check, delete and hide the EHR of patient without his permission. Therefore, the preservation of patient's private data must be carefully protected.

In nowadays hospitals, the integration of intelligent systems IoT aims to improve the quality of patient's medical life, and to decrease his suffering. The smart hospital (SH) is adding the intelligence to traditional hospital system. It covers all resources and locations with the patient information (Magdy, 2013). This intelligence is expressed the effective use of technology as RFID (radio frequency identification), medical equipment must incorporate RFID tags placed by the manufacturer, and contain a standard unique identifier. The doctors, nurses, caregivers and hospital staff wear an authentication means, that stores their employee ID number (Fuhrer and Guinard, 2006). At the arrival of a new patient, a new EHR with an integrated automatic storage, RFID tag is created, a room for a medical stay is reserved if necessary. The patient receives a bracelet to store his personal information (e.g., digital photo, unique patient code, etc.), and link it with his medical record.

With the advance of new communication technologies and the use of wearable embedded technologies in mobile networks, distance monitoring of health status has become possible, in order to provide the medical support outside of hospital and specifically at home, in particular, the smart homes are designed for the dependent and aged people who prefer to live in more safety, more autonomy and in high quality health condition (Aloulou et al, 2013). Remote monitoring of the patient's health state makes his EHR available at any time and any location. It gives the ability to have more details in relation of patient's private life.

The mobile networks and ubiquitous devices favored the emergence of detection technologies. They monitor automatically and preventively the health conditions. Moreover, they detect any undesirable situation affecting the health private data of patients. The EHR is a central element in smart hospital. All inside or outside threats can access to various mobile

health devices. They electronically treat the private data of patient may aim at his privacy. Furthermore, the current developments in sensor networks, actuators, RFID technology, and mobile computing show the limitations of devices in terms of resources such as energy, storage capacity, calculation and bandwidth.

The SH environment is composed of heterogeneous devices, which constantly exchange different information. In the context of this work, the security application within a smart hospital is in the category of personal and home: at the scale of personal, home and healthcare (Ouaddah et al, 2017). The EHRs enable patients to access, manage, and share certain of their own health information. The health bodies are able to diagnose the status of patients. They read their EHRs in SH system to ensure the reliable communications exchanging sensitive information between the trusted devices, including the CHDO and the wearable device SBO. The main problems with smart care environments are related to information flow, patient's data storage and other entities in the health care system. These problems are classified: Unauthorized access and privacy of health information. The privacy is the divulgation of personal information of patient (PIP), such as last name, first name, birth date, phone number, address, social security number (SSN), etc. A violation of health information of patients (HIP), such as reports of additional examinations (biology, radiology, imagery, medical notes and results of consultation, etc.) and disclosure of patient medical secrets, such as details of his illness. The smart hospital requires the highest level of data confidentiality, and this applies especially for wireless medical devices. The access control plays an important role in the SH environment, because of the various kinds of users (Wang and Jiang, 2015), that create the need of ability to specify (1) what users may access to different EHRs, (2) what parts of this record, and (3) what kinds of operations may be performed. These requirements are important in order to filter illegitimate access to health data, which could present negative impact on the patient life. This allows also to design a more user-centric access control model, which gives them the total ability to control their wearable devices with specific granularity.

In this study and in order to protect the privacy and integrity of patient's EHR. We propose two protocols, the first one is a context-aware pseudonym service. It protects the patient's personal and health information in an intelligent space, that equipped with miniaturized and not miniaturized embedded technology. In addition, we prevent the disclosure of the patient's location during his hospital stay. The second is an authorization protocol. It controls the using and sharing of health information. Moreover, this protocol monitors the actions and interactions of doctor with the patient and his connected objects, including the access rights to examine and obtain a copy of EHR under the resource constraint. The authorization protocol uses the context to generate a set of roles with assigning their trust values. One role is activated at a time if its trust value is greater than or equal to the threshold value. A dynamic delegation mechanism is created to better manage the interactions between health bodies.

The rest of our paper is organized as follows. In Section 2, we review some relevant privacy and access control solutions in the health care environment. In Section 3, we present our system model. In Section 4, we present the description of the proposed security schema. The analysis of our approach is detailed in Section 5. The Section 6 concludes this paper.

2 Related Work

2.1 Privacy in the healthcare

The devices connection in wireless body area network (WBAN) has great advantages in the healthcare. However, it poses the confidentiality problems, that's why, there has been an effort of research for privacy issues in IoT healthcare applications in recent year. In (Li et al, 2012), the authors have proposed a method to encrypt each EHR with one-to-many encryption methods, such as the ABE technique, before outsourcing it. Encryption algorithms such as AES and MD5, together with efficient key management, have been used to encrypt each EHR file. A health system can be divided into two security domains, namely public domains (PUDs) and personal domains (PSDs), according to different user data access requirements. PUDs consist of users who need to access based on their professional roles, such as doctors, nurses and medical researchers. For each PSD, its users are personally associated with a data owner, and they make access to EHRs based on access rights assigned by the owner (AL-mawee, 2012). In (Ukil et al, 2014), the authors have presented a privacy measurement scheme that detects, and analyzes sensitive content of time-series sensor data. It measures the amount of privacy to make a decision whether to release private data or not. (Tajer et al, 2011) have proposed a framework that guarantees detection of the cyber attacks, and recovering from them. Different controlling agents, distributed across the network, constitute the attack detection subsystem. System recovery involves iterative local processing and message passing. In (Li et al, 2011), the authors have proposed rolling-code cryptographic protocols, and body-coupled communication. These protocols aim to mitigate the eavesdropping on disabled's health data. The study in (Haas et al, 2011) is a privacy-management system. It offers informational self-determination to patients, including usage control with implicit possibility to trace data flows after sensitive data has been legitimately disclosed. The proposal mainly consists of two parts:(a) A trustworthy central EHR system. (b) A modified digital watermarking scheme. They control data flows after disclosure. This approach offers a user-controlled disclosure of health data to third parties. It does not force the patients to trust the EHR system provider. Additionally, it offers the ability to override policies in the case of an emergency. In this case, the patient (or e.g. the patient's general practitioner) is notified and legal action might be taken. It creates an attested third party (ATP). In contrast to a trusted third party (TTP), users of an ATP do not have to trust the provider of TTP, the system can prove its behavior towards a verifier. An ATP offers the advantages of secure processing. It stores also the sensitive data without altering the trust model. The system for EHRs is divided into two subsystems: The patient service and the data service. The data service controls the disclosure and storage of EHRs. The service of patient offers administrative communication. It is an interface for patients to system, where they can express privacy policies on the usage of their data, and check their enforcement. In (Atzori et al, 2010), the authors have presented a conceptual design and a prototype implementation of a system based on IoT gateways, which aggregate health sensor data, and resolve privacy issues through digital certificates and PKI data encryption. (Yang et al, 2017) have proposed a reliable, searchable and privacy-preserving e-healthcare system, which takes advantage of emerging cloud storage and its infrastructure. It enables the healthcare

service providers (HSPs) to realize remote patient monitoring in a secure, and regulatory compliant manner. This system is built upon a novel dynamic, searchable symmetric encryption scheme. It prospects and verifies the delegation of health data generated periodically. While the forward privacy is achieved by maintaining an increasing counter for each keyword at an IoT gateway. The data owner delegated verifiability comes from the combination of the bloom filter and aggregates message authentication code. (Wang et al, 2015, 2017, 2018) have constructed a secure proxy re-encryption (PRE) based on Cramer-Shoup encryption. They have designed a secure E-health cloud system framework based on IBE. They have proposed also a scalable and controllable cloud data sharing framework for cloud users based on dual of proxy re-encryption scheme. In (Hall et al, 2013), the authors can guarantee protecting records by using differential privacy techniques, which rely on adding noise to patient records. (Martínez et al, 2013) have proposed a general framework that enables the anonymization of structured non-numerical medical data from a semantic perspective. The framework formalizes three operators (comparison, aggregation and sorting). It exploits medical knowledge structures to enable a semantically-coherent managing of medical terms. Afterwards, the framework is used to adapt three well difference statistical disclosure control (SDC) methods. It masks sensitive attributes while preserving, up to a certain degree, so that structured non-numerical data could be k-anonymised.

2.2 Background and literature related to access control

A complete access control infrastructure covers the following three functions (Suhendra, 2011): Authentication, authorization and accountability. We focus on authorization function. However, we leave the authentication and accountability out of the scope of our work. The authorization comprises following phases (Ouaddah et al, 2017): Define a security policy (set of rules), select an access control model to encapsulate the defined policy, and implement the model. In (Benferhat et al, 2016), the authors have proposed a security policy analysis, that involves actions with different levels of granularity. They then show how to integrate complex actions into access control models. They consider complex actions as a partial pre-order of (a_i, o_j), where a_i is an elementary action and o_j is a concrete object. (Wang and Jiang, 2015) have developed a task-based access control model (T-RBAC) for a healthcare medical environment. The T-RBAC introduces concept of task by dividing them into four categories: inherited tasks, non-inherited tasks, passive tasks, and active tasks. In RBAC, the roles are assigned statically by the system administrator. In which access is controlled based on the roles that users have in a system (Jayant et al, 2014). In (Aftab et al, 2015), the authors have introduced a new model by merging ABAC and RBAC in order to enjoy the benefits of both models and to cover their deficiencies. (Hong-Yue et al, 2012) have investigated the impact and functions of context factors in access control policy decision, and have proposed a context-aware fine-grained access control model. In (Sujansky et al, 2010), the authors have described the design and implementation of an access-control mechanism for PHR repositories, that is modeled on the eXtensible Access Control Markup Language (XACML) standard. (Zerkouk et al, 2013) have presented a novel adaptable access control model and its related architecture. The security policy is based on the handicap situation analyzed from

the monitoring of user's behavior, in order to grant a service using any assistive device within intelligent environment. In (Bernabe et al, 2016), the authors have proposed a flexible trust-aware access control system for IoT (TACIoT), which provides an end-to-end and reliable security mechanism for IoT devices, based on a lightweight authorization mechanism and a novel trust model that have been specially devised for IoT environments. (Rivera et al, 2015) have applied a schema that unifies access control systems between intelligent agents, IoT devices and hybrid elements. This schema tries to seamlessly apply access control policies independently of the nature of entities, that interact in an IoT environment.

In an intelligent healthcare system, a dynamic access control model must meet the following criteria: The **integrity and confidentiality** refer to the fact that an unauthorized user can not read and not write to the controlled information (Smari et al, 2009, 2014). Any attempt to falsify or disclose patient data can cause fatal damage, such as incorrect diagnosis or even death. Also, the restricted access to home devices is also necessary in case of remote consultation. The need of **granularity** represents the level of detail, and expressive of the grammar used to specify, formulate and apply the security policy in order to properly evaluate the decision, grant or refuse the access of health body to SBO. The **revocation** is ability to revoke the access permission to resources of patients, including its sensors and SBO. So, the health organization no longer has access to allocated resources if its generated role is revoked. The **delegation** is widely recognized as an important mechanism, it ensures elasticity and flexibility in the assignment of tasks to authorized users or roles, especially in the event of resource constraints, urgent delays (Priya et al, 2014), so that a user can grant access rights or some of the rights granted to another subject (Ouaddah et al, 2017). Delegation typically involves two users, a delegator and a delegate. This could involve an elementary authorization, a role, or even a role hierarchy. It may be permanent or temporary, based on grants (delegate retains delegated authority), or transferred (delegate loses delegated authority during delegation depending on context) (Priya et al, 2014). The **reliable availability** is an important criterion in smart hospital. The EHRs are not available for unauthorized health bodies. In the event of absence or delay of a health actor, a level of availability is essential for delegate to ensure the urgent interventions, and guarantee the continuity of healthcare services. In the **flexibility,** the access control must be adaptable to different contexts. In addition, it should support longevity and planned models, as well as spontaneous and short-lived causal interactions (Ouaddah et al, 2017). Indeed, collaboration between the health bodies in a smart hospital is established implicitly and not scripted. The role of service provider (health actor), or service consumer (patient) is generated dynamically according to the context, since it can be played alternately by the same entity. In the **usability,** the SH and home health services are managed by non-expert users (health body, hospital staff, patient). The access control should be easily managed, expressed and modified. It is important that the access control system involves users, with their different competencies in the authorization policy, and facilitates their spontaneous and autonomous interaction with the security system. In the **user oriented,** the users are the master of their own data, they have full and granular access. In SH, patients are the pivotal element, because their EHRs are considered the fuel of any healthcare application. The access authorization model that targets this type of application is strongly required to be user driven, and to

preserve their privacy (Ouaddah et al, 2017). In the **decentralization,** the smart hospital contains a set of entities. Sharing and access to information between them must be done directly, without the intervention of a trusted third party. The **scalability** is the capacity of the access control model to adapt to the evolution of users, because of the potentially unlimited number of resources (sensors, miniaturized and non-miniaturized devices), and subjects (health body). The authorization mechanism should be scalable in size, structure, and number of users and resources (Ouaddah et al, 2017). In the **heterogeneity,** the SH is a collaborative environment that combines multiple technologies and devices. A standard layer should be designed to achieve overall agreement. It ensures effective dialogue between all entities that make up the system. In the **lightweight,** the resource constraint of wearable devices poses always the access control problems. Our authorization model supports light solutions such as solution based on elliptic curves. The environment of smart hospital is rich in terms of contextual information (vital signs sensors, wearable devices, environmental sensors, CHDO, SBO, etc.), that provides health services of dynamic context-aware of patient (personal and health information, tasks, access schedule, organization, device context, etc.), and his environment. The **trust** is the degree that a subject will accomplish as expected in a given context (Smari et al, 2009, 2014). The concept of trust has already been used in access control (Liu, 2008). A subject will be associated with a quantified trust level, which represents the one of its attributes during its interventions in the object.

We give a comparison of the related work, which is presented in Table 1. We classify the properties into two main classes, the first is the class of security services and the second class is about the access control properties. Most of the works in the literature propose context-based access control policies, such as (Wang and Jiang, 2015; Benferhat et al, 2016; Aftab et al, 2015; Smari et al, 2014; Priya et al, 2014; Hong-Yue et al, 2012; Sujansky et al, 2010; Zerkouk et al, 2013; Bernabe et al, 2016; Rivera et al, 2015). However, no work in the literature did provide the revocation property. Few works guarantee the decentralization, the lightweight processing, delegation, usability and scalability. In addition, (Smari et al, 2014) is the only work that ensures almost of security and access control properties. In the literature, the access control protocols did not provide all the security and access control services, which are highly required in smart hospital environments.

3 System model

3.1 Scenario

Intelligent health care system (IHCS) is based on the use of ubiquitous and intelligent infrastructure, a patient constitutes a wireless body area network (WBAN), in which sensor nodes are placed on the skin or implanted inside the patient's body, that measure a set of physiological phenomena in order to monitor his health continuously. They collect all kinds of medical information as represented in equation 1:

$$\mathsf{BNP_i} = \{< \mathsf{S_k},\ \mathsf{ph_k},\ \alpha_k >, \mathsf{k} = 1 \text{ to } \mathsf{N_i}\} \tag{1}$$

Table 1: Comparative analysis (+: Realized property, -: Unrealized property)

		Literature Works									
		Wang and Jiang (2015)	Benferhat et al (2016)	Aftab et al (2015)	Smari et al (2014)	Priya et al (2014)	Hong-Yue et al (2012)	Sujansky et al (2010)	Zerkouk et al (2013)	Bernabe et al (2016)	Rivera et al (2015)
Security services	Confidentiality & Integrity	-	-	-	+	+	+	-	-	+	+
	Reliable availability	+	+	+	+	+	-	-	-	-	-
	Trust	-	-	-	+	-	+	-	+	+	-
Access control properties	Granularity	-	+	+	+	-	-	-	+	-	-
	Revocation	-	-	-	-	-	-	-	-	-	-
	Delegation	+	-	-	-	-	-	-	-	-	-
	Flexibility	-	-	+	+	-	-	+	+	+	-
	Usability	-	-	+	-	-	-	-	+	-	-
	User Oriented	+	-	-	+	-	-	+	+	-	-
	Decentralization	-	-	-	+	-	-	-	-	-	-
	Scalability	-	-	-	+	-	-	-	-	+	-
	Heterogeneity	-	-	-	+	+	-	-	+	+	+
	Lightweight	-	-	-	-	-	-	-	-	+	-
	Context Awareness	+	+	+	+	+	+	+	+	+	-

Where $\mathsf{BNP}_{\mathtt{i}}$ denotes the body network of patient $\mathtt{i}$, $\mathsf{S}_{\mathtt{k}}$ is the sensor $\mathtt{k}$, $\mathsf{ph}_{\mathtt{k}}$ represents the phenomenon measured by the sensor $\mathtt{k}$ and $\alpha_{\mathtt{k}}$ represents the value or the interval of normal values measured by the sensor $\mathtt{k}$. The system administrator is responsible for defining the phenomena measured by each sensor as well as their normal values, for example, Salah is a patient, he is controlled by three sensors, oxygen in blood sensor, blood glucose sensor and body temperature sensor. The body network of Salah $\mathsf{BNP}_{\mathtt{salah}}$ is represented as follows:

$$\mathsf{BNP}_{\mathtt{Salah}} = \left\{ \begin{array}{l} < \mathsf{S}_1,\ \mathtt{Oxygen\ in\ Blood},\ [95\,\% - 100\,\%] >, \\ < \mathsf{S}_2,\ \mathtt{Blood\ Glucose},\ [72\ \mathtt{mg/dL} - 108\ \mathtt{mg/dL}] >, \\ < \mathsf{S}_3,\ \mathtt{Body\ Temperature},\ 37^{\circ} >, \end{array} \right\} \tag{2}$$

The admission procedure of new patient begins with the creation of his EHR. This last is stored in the hospital's central server database (SDB). The EHR monitors and registers the health status of patient. Each patient receives a smart bracelet object (SBO), which plays the role of a local collection point and guidance in urgent situations. The patient's personal information and his EHR are stored in SDB, while the updates from the different sensors are stored locally in a smart bracelet object database (SBODB), before transferring them to central database as well as the authorized health body. Each element of the health body receives an authentication means, that stores their static and dynamic contexts using it at the entrance and exit of smart hospital. The doctor must also have an overall collection point in the form of a control health device object (CHDO), it can interact with SBO via the Internet

connection and IoT network. The doctor also uses a local database to collect, manage and store the status of his patients. The authorized health body can access the patient's medical and personal information, and authenticate according to patient's context (health state, place and time of consultation). Furthermore, the sensors placed on the patient's body, the set of monitoring and control equipments place inside the intelligent home to simplify patient privacy, they are connected via the Internet with the hospital system on one side and the patient via his SBO on the other side. The patient can communicate with his doctor to give him the necessary prescriptions. If a hospital stay is necessary, he resides in a room equipped with health facilities, the consultation is according to his health state. Our system model is illustrated in figure 1.

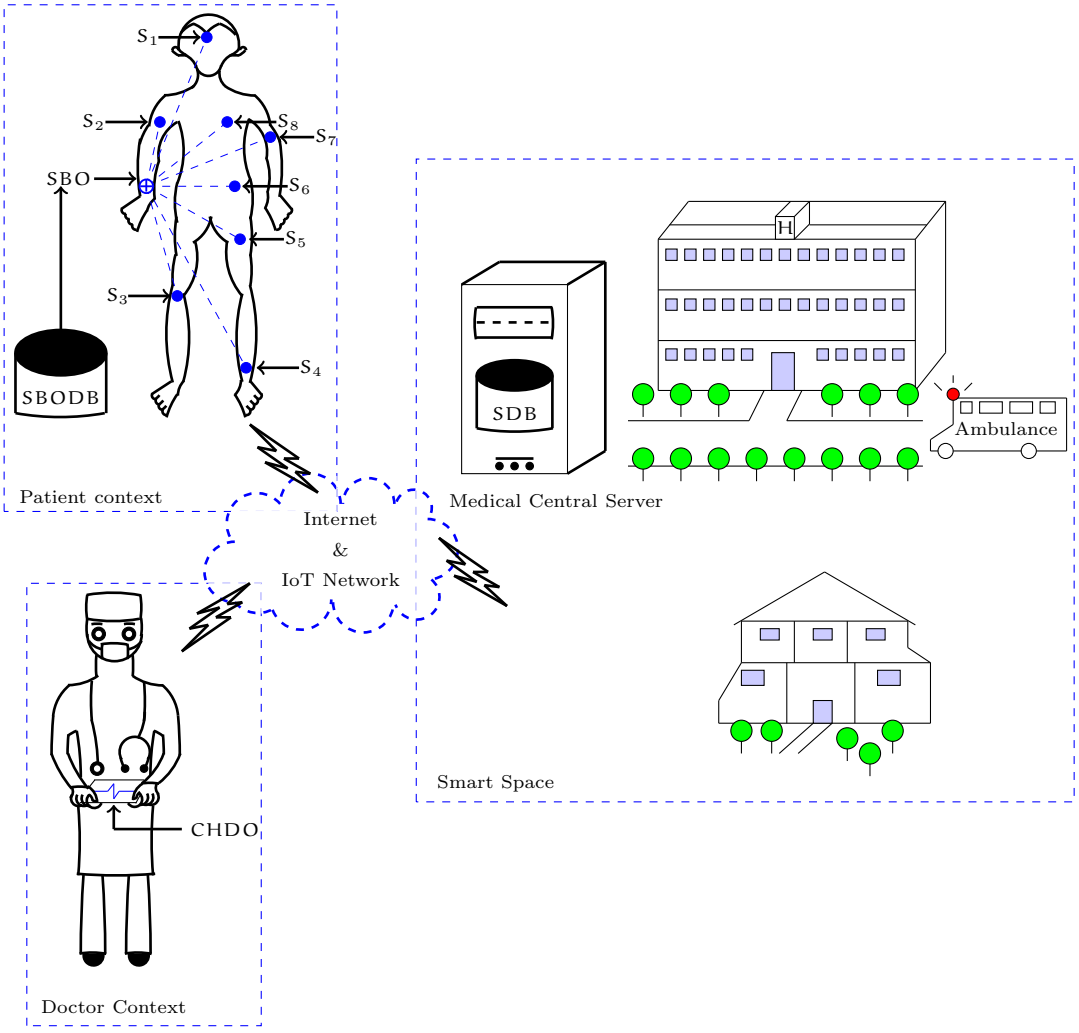

Fig. 1: System model

3.2 Assumptions

Our smart hospital system assumed that the SBO is responsible for the managing communication security in the WBAN. The SBO sends information to the doctor in an urgent case via the IoT network. The health bodies may periodically follow the patient's health status.

Their access rights to the patient are recorded at the SBO and possibly in SDB. The patient can monitor his health state at the hospital (visit consultation, hospital stay), or in the smart home (remote consultation), his EHR is registered in a hospital data base with access rights.

4 Proposed security scheme

4.1 Privacy protocol

4.1.1 Preliminaries

The context is any information that can be used to characterize the situation of an entity (person, place, object) (Dey, 2001), or any information used to characterize the current status of any object or entity (Priya et al, 2014). It is spatial - any information characterizing the situation from spatial dimension (e.g. location, place, position); temporal - any information characterizing the situation from the time dimension (e.g. timestamp, period of day, month, year, day, season); spatio-temporal - any information characterizing the situation that is dependent of both spatial and temporal dimensions i.e. each piece of information is associated with a particular location at a particular time (e.g. weather conditions, temperature, noise, luminosity); social - any information characterizing the situation from social relationships (e.g. nearby persons and nearby friends); and computer - any information describing the situation from the computational characteristics (e.g. user's device capacities) (Filho and Martin, 2009). In our paper, we define the context according to the patient and his health environment:

1. **Static patient context data:** Personal information (patient identifier, social security number, first name, last name, sexe, age, etc.)
2. **Dynamic patient context data:** Medical information such as:
   a) **Health state:** Corresponds to all information related to the physiological state of the patient. It consists of several sub contexts: (i) Physiological context, which is the state of vital signs, corresponds to data emitted from body sensors. (ii) The tasks of health monitoring, that corresponds to all results of medical acts performed on a patient. In our work the tasks are:
      - The set of formalized information collected during the consultation visit, or distance as: prescriptions, medical procedure, symptoms, results of analyzes,
      - The patient's antecedents,
      - The set of formalized information established at the end of the hospital stay,
      - The set of information that was collected from third parties not involved in therapeutic care.

b) **Spatial Context:** This is the location of patient follow-up at a given time. It represented by L illustrated in equation 3:

$$L = \begin{cases} N°Service||N°Room \vee N°Bloc||N°Bed & Hospital\ stay \\ @Home & Distance\ Consultation \\ N°Service[\vee||]N°Bloc & Visit \quad Consultation \\ Not\ Exist & Else \end{cases} \tag{3}$$

c) **Temporal Context:** Refers to the period of consultation (consultation visit, distance remote consultation, and hospital stay) at which the task is performed. It represents also the receipt date of new information related to physiological context.

4.1.2 Notations

Table 2 summarizes the notations used in the proposed privacy protocol.

Table 2: Notations

Notations	**Explanation**
$KSSBO_i$	SBO Private key of patient i
$KPSBO_i$	SBO Public key of patient i
KSD_j	Private key of doctor j
KPD_j	Public key of doctor j
PID_i	Identifier of patient i
$IDS_{(k,i)}$	Identifier of sensor k implanted in patient i
$ISS_{(k,i)}$	Information sending by sensor k of patient i
ISS_i	Information received by patient i and sending by a set of sensors
α_k	Normal value of sensor k
S_k	Sensor k
$CkISS_{(k,i)}$	Sending date of the data $ISS_{(k,i)}$
$CkISS_i$	Sending date of latest data ISS_i
M_i	(PID_i, ISS_i, $CkISS_i$)
$\|\|$	Concatenation operator
$M_{(k,i)}$	($IDS_{(k,i)}$ $\|\|$ $ISS_{(k,i)}$ $\|\|$ $CkISS_{(k,i)}$)
@	Address
N_i	Number of sensors placed on the patient body i
L_i	Location of patient i
$C_{(k,i)}$	Partial context of patient i (attached to sensors k)
C_i	Context of patient i
T_i	Pseudonym expiration time generated by SBO of patient i
MT_i	Medical task of patient i, MT $\in$\{injection, radiology, blood sample, others\}
TS	Time stamp
PIP_i	Personal information of patient i
$\vee$	Logical Operator OR
RN	Random number
$\cdot$	Multiplication Operation
F_P	Finite field of prime number

4.1.3 Protocol steps

In our proposed privacy protocol, a patient must register by the administrative staff, in order to obtain his identifier, which is necessary for the creation of his pseudonym. The pseudonym has an expired lifetime T_i defined by SBO at the time of its generation. Our protocol illustrated in figure 2 consists of following steps:

Step 1: Admission & Registration
The patient presents physically to hospital. He gives his personal information, as well as his EHR in the case where it is a transfer or has antecedents. A smart bracelet is allocated for each patient i. It has a PID_i and a location tag L_i, which directed him to a service. After consultation, the doctor saves the EHR of the patient.

Step 2: Pseudonym Generation
Each sensor k (S_k) sends periodically to SBO via a secure channel its identifier ($IDS_{(k,i)}$), the phenomenon ($ISS_{(k,i)}$), and the date of sending ($CKISS_{(k,i)}$), that represent the message $M_{(k,i)}$. Afterward, the smart bracelet record it. This allows the SBO to play the role of a detector for abnormal situations related to patient, and displays an advice guide according to patient's health status. In emergency cases, a context-aware pseudonym C_i is generated, and sent to appropriate doctor j. The latter sends his certified public key KPD_j to SBO using Elliptic Curve Cryptography (Koblitz, 1987), (Miller, 1986). In our privacy protocol, we use ECC by the definition of cubic equation as follows:

$$y^2 = x^3 + a \cdot x + b, \tag{4}$$

where a, $b \in F_p$, $p > 3$, and $4a^3 + 27b^2 \neq 0$. In our protocol, we consider $a = -4$ and $b = 2$ to get the elliptic curve:

$$y^2 = x^3 - 4 \cdot x + 2. \tag{5}$$

To generate the encryption and decryption keys, we apply the addition principle in elliptic curve. Given two points P_1 and P_2, with the coordinates (x_1,y_1), (x_2,y_2), respectively. The point p_3 with the coordinates (x_3,y_3), represents the addition results, where x_3 and y_3 are defined as follows:

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3) \tag{6}$$

such that

$$x_3 = \frac{(y_1 + y_2)^2}{(x_1 + x_2)^2} + \frac{(y_1 + y_2)}{(x_1 + x_2)} + x_1 + x_2 + a, \tag{7}$$

and

$$y_3 = \frac{(y_1 + y_2)}{(x_1 + x_2)} \cdot (x_1 + x_3) + x_3 + y_1. \tag{8}$$

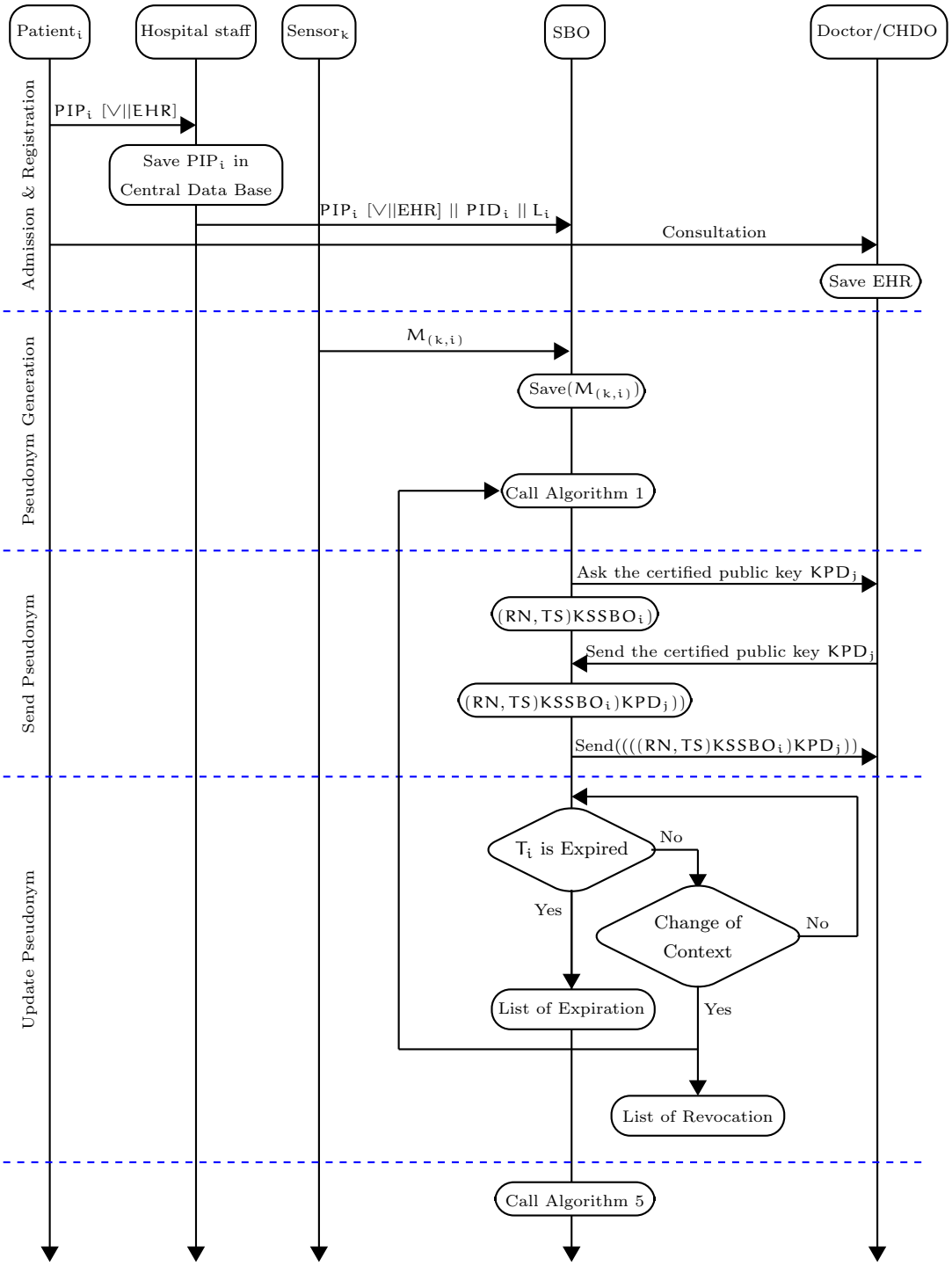

Fig. 2: Sequence diagram of our protocol

The generation principle of public/private key using elliptic curve cryptography is described as follows:

1. In our protocol, the patient and doctor have to agree on a defined curve in equation 5 with a base point Q.
2. Doctor j chooses an integer, which represents his private key $\mathsf{KSD_j}$.
3. Doctor j generates a public key $\mathsf{KPD_j} = Q \cdot \mathsf{KSD_j}$.

4. Likewise, patient $\mathtt{i}$ chooses an integer, which represents his private key $\mathsf{KSSBO_i}$.
5. Patient $\mathtt{i}$ generates a public key $\mathsf{KPSBO_i} = Q \cdot \mathsf{KSSBO_i}$.

The algorithm 1 shows the pseudonym generation method and the intelligent behavior of SBO. The lifetime $\mathsf{T_i}$ of pseudonym is defined at its generation. It is varied according to the type of consultation, the duration between two consecutive medical tasks, or it is a basic time defined by the system administrator. Algorithm 2 illustrates the dynamism of pseudonym generation time.

Algorithm 1: Pseudonym generation

Data: $< \mathsf{S_k}, \mathsf{ph_k}, \alpha_k >$, $\mathtt{k} = 1$ to $\mathsf{N_i}$;
$\mathsf{IDS_{(k,i)}}$;
$\mathsf{ISS_{(k,i)}}$;
$\mathsf{CKISS_{(k,i)}}$;
$\mathsf{KPD_j}$;
Result: Advice guide;
Pseudonym;

```
for Each sensor k do
    if ISS_(k,i) ∉ α_k then
        Show advice guide;
        M_(k,i) ← IDS_(k,i) ‖ ISS_(k,i) ‖ CKISS_(k,i);
        C_(k,i) ← PID_i ‖ M_(k,i) ‖ L_i;
        C_i ← C_i‖((C_(k,i))KPD_j)KSSBO_i;
    else
        for k ← 1 to N_i do
            ISS_i ← ISS_i‖ISS_(k,i);
            if ISS_i is not normal then
                Show advice guide;
                M_i ← PID_i ‖ ISS_i ‖ CKISS_i;
                C_i ← ((PID_i ‖ M_i ‖ L_i)KPD_j)KSSBO_i;
            end
        end
    end
end
Call Algorithm 2;
Save(RN, C_i, T_i);
```

Step 3: Send Pseudonym

During the description of context $\mathsf{C_i}$, the SBO generates a random number RN, and a public/private ECC key pairs ($\mathsf{KPSBO_i}$/$\mathsf{KPSBO_i}$). Afterwards, the SBO signs RN and sending time stamp (TS) by its private key ($(\mathsf{RN}, \mathsf{TS})_{\mathsf{KSSBOi}}$). It encrypts the resulting signature using the doctor's public key ($((\mathsf{RN}, \mathsf{TS})_{\mathsf{KSSBOi}})_{\mathsf{KPDj}}$). The SBO sends the encrypted result to CHDO.

Step 4: Update Pseudonym

Each pseudonym has a period of life. The smart bracelet must obtain a new pseudonym at each change of the patient's context, or after a basic time defined by the system administrator. In the case of a context changing, the expired pseudonym is maintained in a revocation list, otherwise, it will be saved in expiration list after the exhaustion of the allocated time T_i.

Algorithm 2: Time pseudonym

```
if Consultation visit then
    T_i ← Moment of consultation;
else
    if ((Hospital stay) ∨ (Distance consultation)) then
        if MT is changed then
            T_i ← Time of MT_{i+1} − Time of MT_i;
        else
            T_i ← Based time;
        end
    end
end
```

4.2 Authorization protocol

4.2.1 Constructing our authorization model

Our proposed authorization model defines the following components:

1. Attribute (A): It is a variable that captures the properties of an entity i. An attribute record (AR) represents a set of n attributes attached to the same entity.

$$AR_i = \{A_{(i,1)},\ A_{(i,2)},\ \cdots,\ A_{(i,n)}\} \tag{9}$$

   In our authorization model, the system administrator is responsible for assigning attribute values.
2. Context (C): The context aims to manage, and organize the different users, and their hierarchical levels between them according to: Time, environment, organization, and health action:
   - Subject (S): The subject S is the user of access control. In our work, it represents the members of health bodies (HB=doctors and nurses). The attribute record of health body (AR_{HB}) represents a set of n attributes attached to HB:

$$AR_{HB} = \{A_{(HB,1)},\ A_{(HB,2)},\ \cdots,\ A_{(HB,n)}\} \tag{10}$$

   - Control Health Device Object(CHDO): The health body uses the control health device for monitoring and remote consultation of patients. The attribute record of control health device object(AR_{CHDO}) represents a set of n attributes attached to CHDO:

$$AR_{CHDO} = \{A_{(CHDO,1)},\ A_{(CHDO,2)},\ A_{(CHDO,3)},\ \cdots,\ A_{(CHDO,n)}\} \tag{11}$$

– Smart Bracelet Object (SBO): It is the health device assigned to each patient, and manipulated by health body with its resources (file, database, etc.). The attribute record of smart bracelet object (AR_{SBO}) represents a set of n attributes attached to SBO:

$$AR_{SBO} = \{A_{(SBO,1)},\ A_{(SBO,2)},\ A_{(SBO,3)},\ \cdots,\ A_{(SBO,n)}\} \tag{12}$$

– Organization(O): It is a set of health body and their devices that monitor the health state of the same patients. In our paper, we represent the organization of n health body and their objects as follows:

$$O = \{(AR_{HB}, AR_{CHDO})_i,\ i = 1 \text{ to } n\} \tag{13}$$

– Time (T): Every health body can have a schedule to follow his patients. Its attributes record of time (AR_T) is:

$$AR_T = \{Minute, Hour, Day, Month, Year\} \tag{14}$$

– Health Environment (HE): This is the location of health body at a given time. Its attributes record (AR_{HE}) is:

$$AR_{HE} = \{A_{(HE,1)}, A_{(HE,2)}, \cdots, A_{(HE,n)}\} \tag{15}$$

– Health Actions (HA): It represents the operations assigned to a health body on a set of objects of the patient, and this to monitor its health state at a given time, in a given environment, and from a given environment. In our model, the authorized health body can read, write, update or delete the patient resources. Its attributes record (AR_{HA}) is:

$$AR_{HA} = \{A_{(HA,1)}, A_{(HA,2)}, \cdots, A_{(HA,n)}\} \tag{16}$$

3. Role (R): It groups together the privilege set, that will then be assigned to the users. In our work, role definition depends on health body's static context, his devices, health actions, location and trust.
4. Trust Degree (TD): Indicates the authorization value $\in$ [0,1] of the health body on SBO. It takes the value $0 < TD \leqslant 1$ according to context, where the value 1 is fully authorized, and the value 0 is the unauthorized one.

When a message arrives from the SBO to HB, the authorized doctor tries to access the patient to perform the necessary medical actions, according to his received context (see the privacy protocol in Section 4.1). He must provide his context via his CHDO. The architecture of our security policy is shown in figure 3.

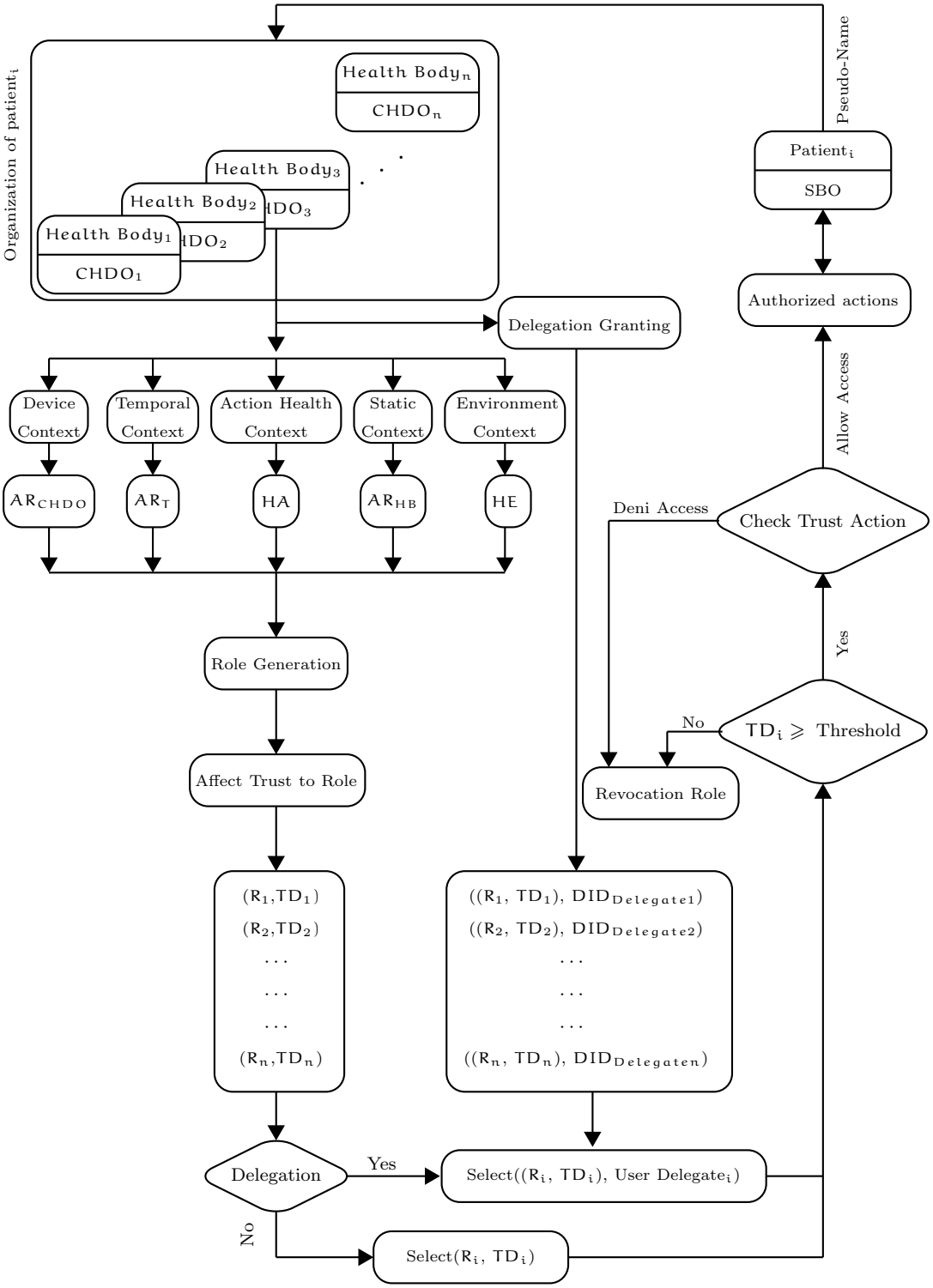

Fig. 3: Authorization and delegation architecture based on TCR (Trust, Context and Role)

4.2.2 Protocol phases

Our authorization protocol consists of three phases, phase I for role generation, from the contextual attributes, we generate a set of dynamic roles for each health body. We take the

doctor as a representative of the health bodies, phase II for trust affectation, each role is attached to a trust value in order to validate the doctor's context attributes, and phase III for delegation role and access authorization, in which assigning the trust values for the delegates if that is the case, then activating the associated role and finally verifying the access privileges.

Phase I: Role Generation

The dynamic generation of contextual role R_C constitutes the set of role R, and depends on attributes AR_i for each health body. The detail of this phase is illustrated in algorithm 3.

Algorithm 3: Role generation

Data: AR_i;
Result: R;
C$\leftarrow$ {};
R $\leftarrow$ {};
for *each entity i* **do**
  C$\leftarrow$ C $\|$ AR_i;
  R$\leftarrow$ R $\cup$ R_C;
end

Phase II: Trust Affectation

Once the set of dynamic roles R_i are generated for each health body, the trust values (α_j) that are assigned to them based on AR_i as illustrated in algorithm 4.

Algorithm 4: Trust affectation

Data: R={R_1, R_2, $\cdots$, R_n} ;
Result: RT={(R_1, TD_1), (R_2, TD_2), $\cdots$, (R_n, TD_n)};
Call Algorithme 3;
RT $\longleftarrow$ {};
for *each* $R_i \in R$ **do**
  $TD_i \longleftarrow 0$;
  for *Each attribute value j* **do**
    $TD_i \longleftarrow TD_i + \alpha_j$;
  end
  RT $\longleftarrow$ RT $\cup$ {(R_i, TD_i)};
end

Phase III: Delegation Role and Access Authorization

After the assignment phase of trust values , if the health body delegates his roles, then, he sends a delegation message to the doctor delegate, including his DID (doctor identifier) with a set of delegated roles and their trust values respectively. Afterwards, only one role is selected by both the delegate or its owner in absence of delegation, if selected role trust value is greater than or equal to a threshold defined by system administrator, therefore, the role is activated otherwise a revocation procedure is launched. Furthermore, the health

body actions performed on SBO vary according to trust value assigned to activated role, for example, write access, update and delete to a file requires a higher trust degree (β) to that in reading (δ), and access to confidential file requires a higher trust degree than that of an ordinary file. The detail of this phase is illustrated in algorithm 5.

Algorithm 5: Delegation role and access authorization

Data: RT=$\{(R_1, TD_1), (R_2, TD_2), \cdots, (R_n, TD_n)\}$;
Result: Role Delegation;
Access Permission;

Call Algorithme 4;
if *Delegation=True* **then**
  Send((R_i, TD_i), $DID_{delegates\ i}$);
end
Select (R_i, TD_i);
if $TD_i \geqslant$ *Threshold* **then**
  if $TD_i \geqslant \beta$ **then**
    Authorization writing;
    Authorization modifying;
    Authorization deleting;
  else
    if $TD_i \geqslant \delta$ **then**
      Authorization reading;
    else
      Unfavorable access;
      Revocation((R_i, TD_i), $DID_i \vee DID_{delegates\ i}$);
    end
  end
else
  Unfavorable access;
  Revocation((R_i, TD_i), $DID_i \vee DID_{delegates\ i}$);
end

5 Analysis of our approach

This section provides the analysis of our approach with two axes. First is the security analysis, where we explain the resistance of our proposed approach against various attacks, in order to show its effectiveness in accordance with the design goals. Next, we provide the practical analysis in terms of pseudonym generation time, storage overhead and response time.

5.1 Security analysis

5.1.1 Privacy preserving integrity

In Step 2 and 3 of the privacy protocol, the generated context-aware pseudonym is signed by the private key (KSSBOi) of SBO. It's certified by the public key ($\mathsf{KPD_j}$) of doctor for verification. In the authorization protocol, an unauthorized user whether a non-delegated doctor, a doctor who does not have an authorized role, or one who has a trust degree value below the threshold ($\mathsf{TD} < \mathsf{Threshold}$) has no right to access the EHR of patient. Therefore, the message integrity is preserved.

5.1.2 Privacy preserving authentication

The privacy protocol aims to sign and certify the context before transferring it to the appropriate doctor. The CHDO should acquire a new pseudonym after a period of time ($\mathsf{T_i}$). In Step 4 of the privacy protocol, the expired pseudonym is maintained in a revocation list. Otherwise, it will be saved in the expiration list after the exhaustion of allocated time $\mathsf{T_i}$. Therefore, it is hard for an attacker to correlate the pseudonym. In the authorization protocol, the doctor or his delegate can't access to the patient's encrypted data, only if he has a trust degree value greater than or equal threshold ($\mathsf{TD} \geqslant \mathsf{Threshold}$). Furthermore, his role R depends on the health body's static context, devices, health actions, location and trust. Therefore, it is difficult that an unauthorized doctor can access to medical and personal information of patient.

5.1.3 Non-repudiation

In steps 3 of the privacy protocol, the sent context-aware pseudonym is signed by the private key ($\mathsf{KSSBO_i}$) of SBO. It is certified by the public key ($\mathsf{KPD_j}$) of a doctor. Therefore, no other patient can diffuse this pseudonym. Moreover, the pseudonym itself contains a current sending time stamp (TS). Therefore, not only the non-repudiation is assured, but the protocol also provides the prevention against replay attack.

5.2 Practical analysis

In this subsection, we analyze the hardware performance required to put in the real practice our approach. Indeed, each wearable sensor k maintains a set of security parameters. It periodically sends its phenomenon $\mathsf{ISS_{(k,i)}}$ to SBO, which in turn generates a pseudonym corresponds to global context $\mathsf{C_i}$, and send it to health bodies. Thereafter, each health body accesses to SBO to guide and control the patient in an emergency situation. Three important criteria are involved in our approach: pseudonym generation time, context storage space in privacy protocol, and the response time in authorization protocol.

5.2.1 Pseudonym generation time requirement

Here, we discuss in terms of time, the computational overhead incurred by the SBO when analyzing the global context $\mathsf{C_i}$, as well as the pseudonym generation. We also analyze, the

computational overhead incurred by the sensor k during the collection of patient's partial context $C_{(k,i)}$, in order to send it to SBO. Moreover, the message $M_{(k,i)}$ is diffused periodically by each sensor k to SBO of patient i. In emergency cases, the SBO generates a pseudonym corresponds to global context C_i, and send it to CHDO of health bodies, thus, the pseudonym generation time varies according to the number N_i of sensor, that communicate with SBO. It depends on the sending date $CKISS_{(k,i)}$ of $M_{(k,i)}$ by the sensor k, the time generation of global context C_i, the checking time of partial context signature and random number.

In practice, the SBO takes 5 ms to verify the abnormal situations of patient, and the time sending from each sensor to SBO requires 5 ms. Following, we suppose the detailed time to process the necessary transactions of pseudonym generation, and send it to CHDO. Figure 4 illustrates the pseudonym generation time according to various IoT sensors. For example, with 100 urgent wearable sensors, the pseudonym time generation does not exceed 14 seconds. Therefore, we note that, this criterion is well adapted to IoT sensors.

a) **Sensor$_k$:**
   $M_{(k,i)} \leftarrow IDS_{(k,i)} \parallel ISS_{(k,i)} \parallel CKISS_{(k,i)}$
   – $IDS_{(k,i)} \parallel ISS_{(k,i)} \parallel CKISS_{(k,i)}$= 5 ms
b) **SBO:**
   $C_{(k,i)} \leftarrow PID_i \parallel M_{(k,i)} \parallel L_i$
   – $PID_i \parallel M_{(k,i)} \parallel L_i$= 5 ms
   $C_i \leftarrow C_i \| ((C_{(k,i)})KPD_j)KSSBO_i$
   – $(C_{(k,i)})KPD_j$= 20 ms
   – $((C_{(k,i)})KPD_j)KSSBO_i$= 20 ms
   – $C_i \| ((C_{(k,i)})KPD_j)KSSBO_i$= 5 ms
   $ISS_i \leftarrow ISS_i \| ISS_{(k,i)}$
   – $ISS_i \| ISS_{(k,i)}$= 5 ms
   $M_i \leftarrow PID_i \parallel ISS_i \parallel CKISS_i$
   – $PID_i \parallel ISS_i \parallel CKISS_i$= 5 ms
   $C_i \leftarrow ((PID_i \parallel M_i \parallel L_i)KPD_j)KSSBO_i$
   – $PID_i \parallel M_i \parallel L_i$= 5 ms
   – $(PID_i \parallel M_i \parallel L_i)KPD_j$= 20 ms
   – $((PID_i \parallel M_i \parallel L_i)KPD_j)KSSBO_i$= 20 ms
   – Generates RN= 5 ms
   – Save(RN, C_i, T_i)= 5 ms
   – $(RN, TS)KSSBO_i)$ =20 ms
   – $((RN, TS)KSSBO_i)KPD_j)$ = 20 ms
c) **SBO → CHDO:**
   – Send($((((RN, TS)KSSBO_i)KPD_j))$= 15 ms

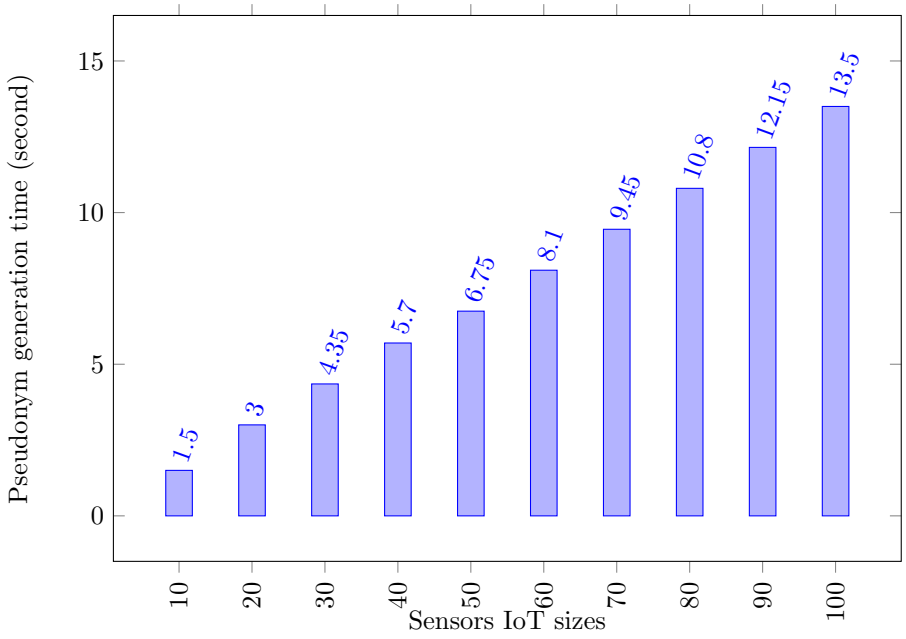

Fig. 4: Pseudonym generation time requirement

5.2.2 Storage overhead

The message $M_{(k,i)}$ sending by each sensor k to SBO of the patient i includes the $IDS_{(k,i)}$, the $ISS_{(k,i)}$ and the $CKISS_{(k,i)}$. Thus, the partial context $C_{(k,i)}$ includes the PID_i of patient i, the message $M_{(k,i)}$ and the location L_i. Moreover, the global context C_i represents the concatenation of signed partial contexts of all sensors, that send the abnormal urgent information to SBO. The following represents the necessary size of context, as well as the total pseudonym size, including the encryption overhead in our proposed privacy protocol. Figure 5 illustrates the storage capacity required according to various IoT sensors sizes. For example, the storage capacity for 100 wearable sensors does not exceed 8500 bytes. Consequently, we note that our proposed protocol presents no constraints in terms of storage capacity.

a) **The message $M_{(k,i)}$:**
   $M_{(k,i)} \leftarrow IDS_{(k,i)} \parallel ISS_{(k,i)} \parallel CKISS_{(k,i)}$
   - $IDS_{(k,i)}$=5 bytes
   - $ISS_{(k,i)}$=15 bytes
   - $CKISS_{(k,i)}$= 5 bytes

b) **The partial context $C_{(k,i)}$:**
   $C_{(k,i)} \leftarrow PID_i \parallel M_{(k,i)} \parallel L_i$
   - PID_i= 5 bytes
   - $M_{(k,i)}$=25bytes
   - L_i= 5 bytes

c) **The message M_i:**
   $M_i \leftarrow PID_i \parallel ISS_i \parallel CKISS_i$
   - ISS_i= 20 bytes

d) **The global context C_i:**

$C_i \leftarrow C_i \| ((C_{(k,i)})KPD_j)KSSBO_i$

– $(C_{(k,i)})KPD_j$=20 bytes

– $((C_{(k,i)})KPD_j)KSSBO_i$= 20 bytes

$C_i \leftarrow ((PID_i \parallel M_i \parallel L_i)KPD_j)KSSBO_i$

– $(PID_i \parallel M_i \parallel L_i)KPD_j$=20 bytes

– $(PID_i \parallel M_i \parallel L_i)KPD_j$= 20 bytes

e) **The pseudonym:**

– RN= 10 bytes

– T_i= 5 bytes

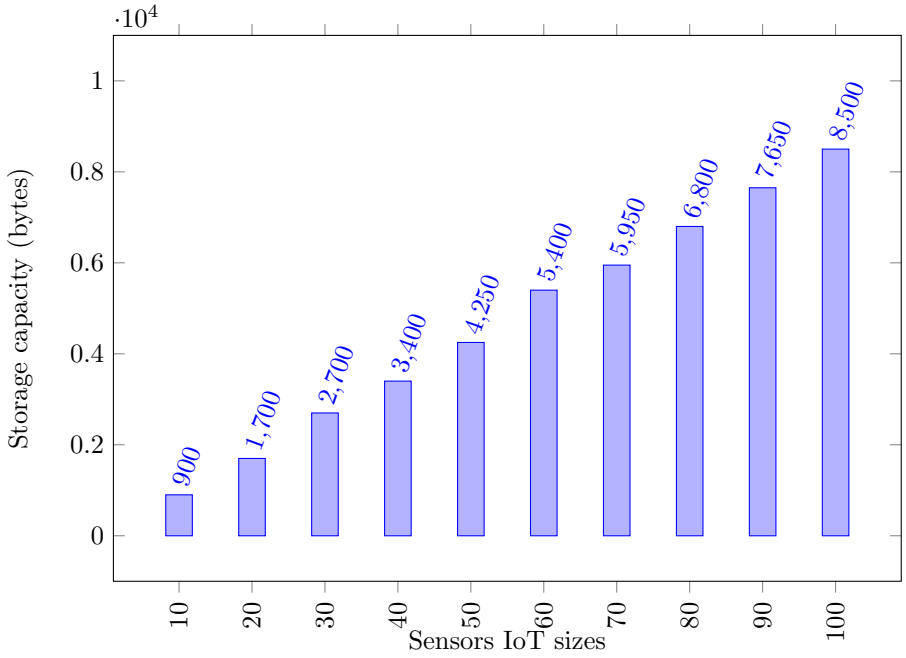

Fig. 5: Storage requirement

5.2.3 Response time requirement

We were interested in the response time, which is highly required in emergency healthcare applications. The generated pseudonym is stored in the SBO, and sent to health bodies who try to decrypt the contents of receiving pseudonym, in order to access to their contexts that contains the information about the patient's situation. After the verification of the delegation, the role selection and the assignment of its trust degree. The SBO only allows legitimate health bodies to access to its resources, and monitor the health status of their patients. In our protocol, we assume a delay time $\triangle^t = 20$ ms, which represents the time lost for each health body to access to SBO. The equation 17 illustrates the calculation of the response time R^t of each access request.

$$R^t = \triangle^t + R * V^t + R^{leg} * T^p \tag{17}$$

where R is the number of access requests from the health bodies to SBO, V^t is the verification time of the delegation, the role selection and the assignment of its trust degree, it can reach

30 ms, R^{leg} is the access requests number of legitimate health bodies trying to access to SBO, and T^{p} is the processing time required to decrypt the pseudonym, in order to access the global context, and find the partial context of each IoT sensor. In our protocol, we assume that T^{t} requires 100 ms. Figure 6 illustrates the response time according to the access request number R^{leg}. For example, with 100 requests, the response time required does not exceed 14 seconds. Therefore, we note that our authorization protocol presents no constraints in terms of response time.

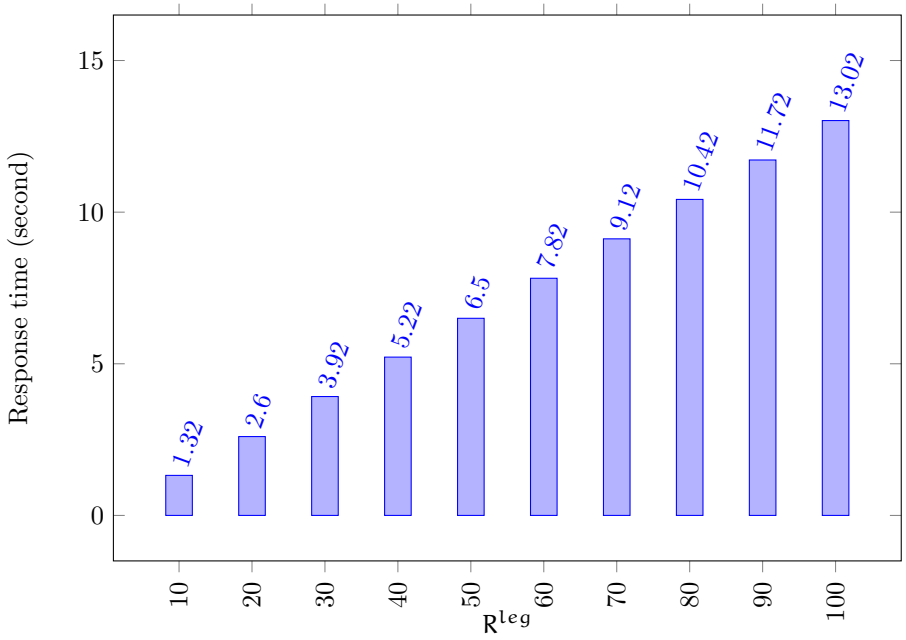

Fig. 6: Response time requirement

6 Conclusion

The use of miniaturized and not miniaturized devices in a smart hospital improve the quality of patient's medical life. However, this environment poses many security problems due to the resource constraints of these devices, taking into account the different living spaces of the patient. The protection of patient data has a primordial importance in the establishment of his EHR record. The specificity of data contained in this record, and the transmission of sensitive information that contains it require the development of a set of security mechanisms, that protect both privacy and access control to this file. In this paper, we proposed an approach based on two new protocols. Firstly, we presented a context-aware pseudonym, that protects the EHR of a patient in hospital, and at home in the case of remote consultation. In addition, we prevented the disclosure of the patient location during his hospital stay. Secondly, we developed an authorization model, which oversees the actions and interactions between the patient's organization and his SBO. The model uses context to generate a set of roles by assigning them trust values. Only, one role is activated, if its trust value greater than or equal to trust threshold assigned to a patient's context. A dynamic delegation mechanism is created to better manage the interactions between health bodies. The practical analysis of our approach shows the acceptable storage and computation overhead.

For the continuity of this work, we aim to extend our privacy protocol by incorporating an efficient mechanism of distributed public-key certificate, taking into consideration a case study under a telemedicine platform. We will propose an information flow control protocol for wearable objects in smart environments.

References

Aftab MU, Habib MA, Mehmood N, Aslam M, Irfan M (2015) Attributed role based access control model. In: Conference on Information Assurance and Cyber Security (CIACS) pp 83–89, DOI :10.1109/CIACS.2015.7395571

AL-mawee W (2012) Privacy and security issues in iot healthcare applications for the disabled users a survey. Master's Theses, Western Michigan University p 651, URL :https://scholarworks.wmich.edu/cgi/viewcontent.cgi?article=1661&context=masters_theses

Aloulou H, Mokhtari M, Tiberghien T, Biswas J, Phua C, Lin JHK, Yap P (2013) Deployment of assistive living technology in a nursing home environment: Methods and lessons learned. In: Journal of BMC Medical Informatics and Decision Making 13(1):42, DOI :https://doi.org/10.1186/1472-6947-13-42

Atzori L, Lera A, Morabito G (2010) The internet of things: A survey. In: Journal of Computer Networks 54(15):2787–2805, DOI :https://doi.org/10.1016/j.comnet.2010.05.010

Benferhat S, Tolba M, Tabia K, belkhir A (2016) Integrating non elementary actions in access control models. In: Proceedings of the 9th International Conference on Security of Information and Networks pp 28–31, DOI :10.1145/2947626.2951960

Bernabe JB, Ramos JLH, Gomez AFS (2016) Taciot: multidimensional trust-aware access control system for the internet of things. In: Journal of Soft Computing 20(5):1763–1779, DOI :https://doi.org/10.1007/s00500-015-1705-6

Dey AK (2001) Understanding and using context. In: Journal of Personal and Ubiquitous Computing 5(1):4–7, DOI :10.1007/s007790170019

Filho JB, Martin H (2009) A generalized context-based access control model for pervasive environments. In: Proceedings of the 2nd SIGSPATIAL ACM International Workshop on Security and Privacy in GIS and LBS SPRINGL'09 pp 12–21, DOI :10.1145/1667502.1667507

Fuhrer P, Guinard D (2006) Building a smart hospital using rfid technologies: Use cases and implementation. In: 1st European Conference on eHealth (ECEH06) URL :https://pdfs.semanticscholar.org/1bc9/43643aa927abd4dc0b40702d8bd239f208ff.pdf

Haas S, Wohlgemuth S, Echizen I, Sonehara N, Müller G (2011) Aspects of privacy for electronic health records. In: International Journal of Medical Informatics 80(2):e26–e31, DOI :https://doi.org/10.1016/j.ijmedinf.2010.10.001

Hall R, Rinaldo A, Wasserman L (2013) Differential privacy for functions and functional data. In: Journal of Machine Learning Research pp 703–727

Hong-Yue L, Miao-Lei D, Wei-Dong Y (2012) A context-aware fine-grained access control model. In: International Conference on Computer Science and Service System pp 1099–1102, DOI :10.1109/CSSS.2012.278

Jayant DB, Swapnaja AU, Sulabha SA, Dattatray GM (2014) Analysis of dac mac rbac access control based models for security. In: International Journal of Computer Applications 104(5):6–13, URL :https://pdfs.semanticscholar.org/45a2/775770d870b8675fb1301919224c9bcb7361.pdf

Koblitz N (1987) Elliptic curve cryptosystems. In: Mathematics of computation Journal 48:203–209, DOI :https://doi.org/10.1090/S0025-5718-1987-0866109-5

Li C, Raghunathan A, Jha NK (2011) Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In: IEEE 13th International Conference on e-Health Networking, Applications and Services pp 150–156, DOI :10.1109/HEALTH.2011.6026732

Li M, Yu S, Zheng Y, Ren K, Lou W (2012) Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. In: IEEE Transactions on Parallel and Distributed Systems 24(1):131–143, DOI :10.1109/TPDS.2012.97

Liu Y (2008) Trust-based access control for collaborative system. In: ISECS International Colloquium on Computing, Communication, Control, and Management pp 444–448, DOI :10.1109/CCCM.2008.203

Magdy SAM (2013) Improve of health care systems for smart hospitals based on uml and xml. In: International Journal of Computer and Information Technology 02(03):484–491, URL :https://ijcit.com/archives/volume2/issue3/Paper020320.pdf

Martínez S, Sánchez D, Valls A (2013) A semantic framework to protect the privacy of electronic health records with non-numerical attributes. In: Journal of Biomedical Informatics 46(2):294–303, DOI :https://doi.org/10.1016/j.jbi.2012.11.005

Miller VS (1986) Uses of elliptic curves in cryptography. In: proceedings of the Conference on the Theory and Application of Cryptographic Techniques CRYPTO 1985: Advances in Cryptology pp 417–426, DOI :https://doi.org/10.1007/3-540-39799-X_31

Ouaddah A, Mousannif H, Elkalam AA, Ouahman AA (2017) Access control in the internet of things: Big challenges and new opportunities. In: Journal of Computer Networks 112:237–262, DOI :https://doi.org/10.1016/j.comnet.2016.11.007

Priya P, Charles PJ, Kumar BR (2014) Context-aware architecture for user access control. In: International Journal of Advanced Research in Computer Science & Technology(IJARCST) 2(3):201–204, URL :http://ijarcst.com/doc/vol2-issue3/ver.2/p_priya.pdf

Rivera D, Cruz-Piris L, Lopez-Civera G, de la Hoz E, Marsa-Maestre I (2015) Applying an unified access control for iot-based intelligent agent systems. In: IEEE 8th International Conference on Service-Oriented Computing and Applications (SOCA) pp 247–251, DOI :10.1109/SOCA.2015.40

Smari WW, Zhu J, Clemente P (2009) Trust and privacy in attribute based access control for collaboration environments. In: Proceedings of the 11th International Conference on Information Integration and Web-based Applications & Services pp 49–55, DOI :10.1145/1806338.1806356

Smari WW, Clemente P, , Lalande JF (2014) An extended attribute based access control model with trust and privacy: Application to a collaborative crisis management system. In: Journal of Future Generation Computer Systems 31:147–168, DOI :https://doi.org/

10.1016/j.future.2013.05.010

Suhendra V (2011) A survey on access control deployment. In: International Conference on Security Technology pp 11–20, DOI :https://doi.org/10.1007/978-3-642-27189-2_2

Sujansky WV, Faus SA, Stone E, Brennan PF (2010) A method to implement fine-grained access control for personal health records through standard relational database queries. In: Journal of Biomedical Informatics 43(5):S46–S50, DOI :https://doi.org/10.1016/j.jbi.2010.08.001

Tajer A, Kar S, Poor HV, Cui S (2011) Distributed joint cyber attack detection and state recovery in smart grids. In: IEEE International Conference on Smart Grid Communications (SmartGridComm) p 202?207, DOI :10.1109/SmartGridComm.2011.6102319

Ukil A, Bandyopadhyay S, Pal A (2014) Iot-privacy: To be private or not to be private. In: IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) pp 123–124, DOI :10.1109/INFCOMW.2014.6849186

Wang P, Jiang L (2015) Task-role-based access control model in smart health-care system. In: MATEC Web of Conferences 22:01,011, DOI :https://doi.org/10.1051/matecconf/20152201011

Wang XA, Ma J, Yang X (2015) A new proxy re-encryption scheme for protecting critical information systems. In: Journal of Ambient Intelligence and Humanized Computing 6(6):699–711, DOI :https://doi.org/10.1007/s12652-015-0261-3

Wang XA, Ma J, Xhafa F, Zhang M, Luo X (2017) Cost-effective secure e-health cloud system using identity based cryptographic techniques. In: Future Generation Computer Systems 67:242–254, DOI :https://doi.org/10.1016/j.future.2016.08.008

Wang XA, Xhafa F, Ma J, Barolli L, Ge Y (2018) Pre+: dual of proxy re-encryption for secure cloud data sharing service. In: International Journal of Web and Grid Services 14(1):44–69, DOI :https://doi.org/10.1504/IJWGS.2018.088394

Yang L, Zheng Q, Fan X (2017) Rspp: A reliable, searchable and privacy-preserving e-healthcare system for cloud-assisted body area networks. In: IEEE International Conference on Computer Communications (INFOCOM) DOI :10.1109/INFOCOM.2017.8056954

Zerkouk M, Mhamed A, Messabih B (2013) A user profile based access control model and architecture. In: International Journal of Computer Networks & Communications IJCNC 5(1):171–181, DOI :10.5121/ijcnc.2013.5112