Toward Energy-Efficient and Trustworthy eHealth Monitoring System

Ajmal Sawand[1], Soufiene Djahel[2], Zonghua Zhang[3], Farid Naït-Abdesselam[1]

[1] Paris Descartes University, Paris, France
[2] University College Dublin, Dublin, Ireland
[3] TELECOM Lille, France

Abstract: The rapid technological convergence between Internet of Things (IoT), Wireless Body Area Networks (WBANs) and cloud computing has made e-healthcare emerge as a promising application domain, which has significant potential to improve the quality of medical care. In particular, patient-centric health monitoring plays a vital role in e-healthcare service, involving a set of important operations ranging from medical data collection and aggregation, data transmission and segregation, to data analytics. This survey paper firstly presents an architectural framework to describe the entire monitoring life cycle and highlight the essential service components. More detailed discussions are then devoted to {\em data collection} at patient side, which we argue that it serves as fundamental basis in achieving robust, efficient, and secure health monitoring. Subsequently, a profound discussion of the security threats targeting eHealth monitoring systems is presented, and the major limitations of the existing solutions are analyzed and extensively discussed. Finally, a set of design challenges is identified in order to achieve high quality and secure patient-centric monitoring schemes, along with some potential solutions.

Keywords: eHealthcare; wireless body area networks; cyber physical systems; mobile crowd sensing; security; privacy by design; trust.

I. INTRODUCTION

The recent advances in wireless sensing technology have led to the emergence of a wide range of applications in different domains such as medical, sports, consumer electronics, social networking, and enterprise usage. Among those emerging applications, eHealth is recognized as the most important and promising one due to its potential for health monitoring of chronic illnesses, lifesaving in emergency situations, and its ability to provide round the clock healthcare to rural and disadvantaged areas. In particular, wireless Body Area Networks (WBANs) are the key enablers of remote and in-hospital health monitoring and are expected to revolutionize the health and real-time body monitoring industry. However, WBANs technology alone is not sufficient to achieve the ultimate goal of eHealthcare stakeholders, and other advanced technologies such as Internet of Things (IoT) and cloud computing are needed to further improve the eHealth monitoring system efficiency.

Thanks to the advancements of Internet of Things, machine-to-machine (M2M) communications are enabled and getting pervasively available. Meanwhile, cloud computing offers plenty of opportunities to services providers and users, significantly facilitating computation or storage outsourcing. As one of the results of such technological convergence, med-

This survey paper firstly presents an architectural framework to describe the entire monitoring life cycle and highlight the essential service components.

ical area has profited from recent advances in sensors design and wireless communication technologies. In particular, the constant miniaturization of electrical devices has empowered the development of e-health monitoring. These include various types of medical and non-medical sensors embedded in smartphones, wearable devices in, on or around the patients' bodies, working as important elements of wireless body area networks, or WBAN in short. Despite the recent technological advancements of WBANs, as well as their great potential to improve the quality of health monitoring, the performance with respect to energy efficiency, privacy and security is not sufficiently guaranteed.

Recent years have witnessed a fast development of smartphones sensors, body sensors and wireless communications, which pave a way for efficient health monitoring. The health care tasks are therefore shifted from traditional clinical environment to pervasive user friendly environment. Also, the range of monitoring subjects could be significantly expanded, varying from the patients at urgent care, e.g., in ambulance, to those with chronic diseases. In particular, the body sensors deployed in, on or around the human body, as well as the context-aware sensors like the ones embedded in smartphones, can be used to measure the fundamental health parameters or vital signs such as heartbeat, temperature, blood pressure. Moreover, other IoT sensors deployed in smart homes or at hospital rooms might provide additional valuable information about the environment where the monitored patient is located, such as the temperature, the level of humidity, the lighting as well as the level of patient's sweat which can be measured by advanced smart beds etc., allowing the medical stuff to achieve more accurate diagnosis and thus deliver more efficient treatment.

For better illustration, an overall eHealth monitoring framework is given in Figure 1, which contains the following major components,

- *Situational awareness sensors*: ranging from implantable devices and wearable sensors to IoT sensors or smartphone sensors, collecting data of interest from the patient and transmitting them to the base station (also called personal servers or gateways for different illustrations purpose);
- *Communication networks*: these include short range wireless communications of WBAN (inter-WBAN communications), WBAN-IoT communications, IoT-IoT communications, as well as various relaying networks (connecting base station with cloud servers) and access networks (enabling clinicians to remotely access data servers) like 3G and wireline networks.
- *Medical data processing servers*: the data is usually stored and processed in remote cloud data centers, which must ensure secure and privacy-preserving computation and storage. In addition, advanced data analytics tools might be applied to derive useful knowledge from the stored data, which can be further leveraged for different purposes.
- *Clinic terminals*: the end users could be nurses, doctors or any other physicians, who will retrieve the medical information from cloud data centers via various access equipment that could be deployed in hospitals, clinics, ambulances or any medical care centers.

It is clear that the quality of eHealthcare

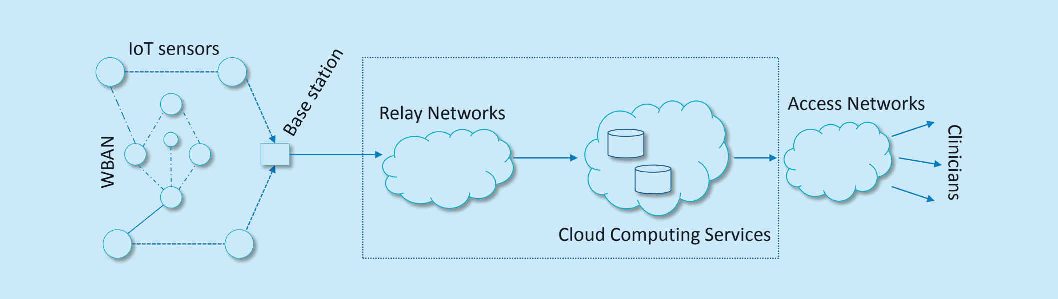

Fig.1 *Cyber-physical system architecture for eHealth monitoring*

service relies on the seamless integration of the above essential components, each of which is attracting tremendous efforts from both academia and industry. For example, WBAN IEEE standard has been released in 2012 [31]. In addition to wireless communications technologies, energy efficiency and patient privacy are always among the top concerns of eHealthcare services. Based on the contributions from different relevant research fields, this paper intends to investigate the key challenges for achieving reliable, efficient and secure patient monitoring, which we argue that it deserves more efforts than it currently receives. We specifically examine a variety of solutions tackling those identified challenges and ultimately propose the potential integrations of those multidisciplinary approaches for constructing a holistic eHealtcare-oriented, patient-centric, Cyber-Physical System (CPS) framework.

In the rest of this paper, we will firstly discuss in detail the major service components in Section II, with main focus on WBANs and crowd sensing. An illustration of potential applications of the proposed monitoring framework is presented in Section III, followed by a description of the tradeoff between performance goals and security of the eHealth Monitoring System in Section IV. Next, security and privacy requirements for designing such a system are described, and a taxonomy of the security threats targeting it along with the existing solutions are discussed, in Sections V and VI, respectively. A set of technical challenges for designing efficient and secure patient monitoring framework is then investigated in Section VII, highlighting the tradeoff between energy efficiency and security issues. In Section VIII, we then study the potential approaches to tackling those identified challenges, and examine their feasibility and effectiveness in terms of the key metrics that are essential to the quality and security of eHealthcare monitoring.

II. A Patient-Centric CPS-Based Ehealth Monitoring Framework

As shown in Figure 1, the CPS-based eHealth monitoring framework is composed of four service components enabled by diverse technologies, as well as three key players.

- Patients equipped with wearable devices forming Wireless Body Area Networks (WBANs), smartphone sensors, as well as IoT sensors including both physically distributed sensors and software sensors or virtual sensors. For example, both iPhone 5 and Samsung Galaxy S4 are equipped with multifunctional sensors, as shows in Figure 2.
- Medical service providers whose role is to facilitate the access of clinicians to different medical datasets in the clouds.
- Clinicians using PDAs, laptops, desktop, smartphones, or even dedicated medical devices to access, display and manipulate the stored datasets if such privilege is permitted.

From a functional perspective, the given architecture can be treated as a typical implementation of CPS (Cyber Physical Systems), which consists of physical layers and cyber (or service) layers, well connected by the most advanced networking and wireless communications technologies.

- **Physical layer**: this layer encompasses WBANs and IoT sensors, cloud data centers, as well as those equipment and devices used by medical staff.
- **Service layer**: the dedicated applications, software and services enabled by physical layer and offered to both patients and clinicians, as well as other interested third parties, such as healthcare related research institutions.

Between the layers are wireless communication networks ranging from LTE-A, NFC, WiFi,3G to high-speed wired networks, conveying the medical data from patient side to clinician side, and vice versa, particularly if an adjustment/actuation of the monitoring devices operating parameters or the patient's environmental conditions are needed (e.g. reducing the heat level in a hospital room due to the detected high sweating level of the patient). It is worth noting that such CPS framework can be carried and deployed at home, in workplaces, as well as in hospitals, thereby making

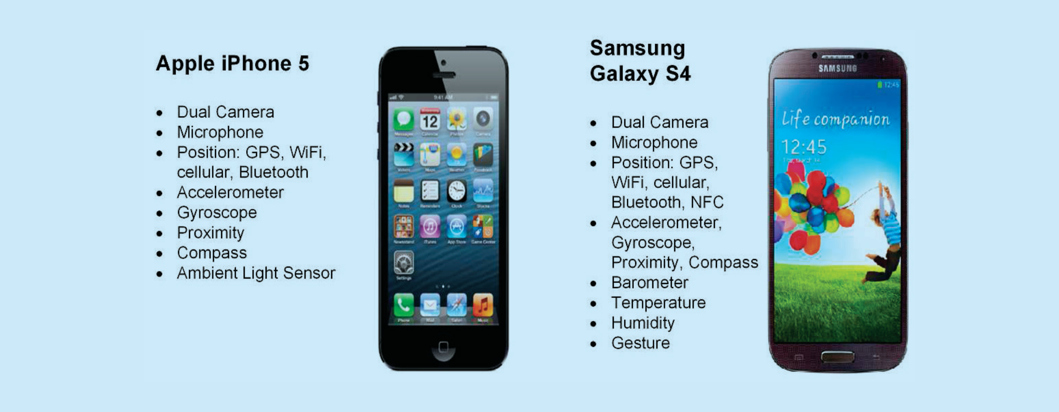

Fig.2 *A rich set of sensors carried by Smartphone*

eHealthchare service pervasively available. However, in this paper, our effort will be dedicated to patient-centric data collection, and we will be specifically discussing WBANs for individual patients and crowd sensing for massive disease monitoring and control.

2.1 WBANs in eHealth monitoring

Usually a WBAN encompasses a number of various sensors, either implanted in the patient's body, on or around the body, together with IoT sensors sensing environmental or contextual information [8]. Those heterogeneous sensors are then integrated through a controller, which creates a link with personal server/smartphone which, in turn, transmits medical data to the cloud either periodically or on demand (i.e. event-driven transmissions). In particular, the Personal Server (PS) application which can run on PDA, smartphone, or home personal computer, is primarily in charge of medical data collection and aggregation, and serves as an interface between WBAN sensors, end users, and other data servers. The PS can also configure and manage WBANs, including sensor nodes registration and initialization (e.g., specify sampling frequency and mode of operation), tasks specification and allocation (e.g., communication channel sharing, time synchronization, scheduling), as well as setting up secure communication channels between the sensors.

Moreover, the PS should be able to assess the patient's health status based on the information periodically collected from the multiple medical sensors, and further detects any abnormal change that may occur. Furthermore, it should be able to apply the required actuation suggested by the medical staff or learnt from knowledge base stored in the cloud. As previously mentioned, PS must establish a secure communication link between WBANs and IoT sensors and medical servers located in the cloud, updating patient information remotely. One concern here is that such a communication link is not always available, so PS is expected to exploit Delay Tolerant Networking (DTN) capabilities, locally stores the data and conduct updates as soon as a communication channel becomes available.

A typical example for illustrating the application of WBANs is emergency care. If a patient who has a heart disease needs an urgent evacuation to the hospital while he is outside for shopping, those implanted or wearable sensors can help to measure the vital signs or physiological signals such as blood pressure, temperature, and heartbeats, and send the corresponding data via personal server to the service center which, in turn, forwards it to the medical staff. As such, the patient's health status can be remotely monitored in real-time, even when he/she is on the ambulance, allowing the doctors to make timely diagnose, and prepare any required tool for the necessary medical intervention/treatment in advance.

2.2 Mobile crowd sensing (MCS) in eHealth monitoring

In addition to individual patient monitoring, observing epidemics at a large scale for efficient diseases prevention and control is also an important function to be accomplished by eHealth monitoring. As one of the novel sensing paradigms recently emerged, mobile crowd sensing or participatory sensing allows ordinary users to contribute their personal data for centralized information gathering and intelligence extraction~\cite{Ganti2011}. Despite those technical challenges in crowd sensing, it has potential to aid doctors or medical researchers in collecting useful data for epidemic studies, so as to further understand the infection and propagation of unknown diseases. To better understand how MCS can be applied to eHealth monitoring, Figure 3 is used to illustrate the basic procedures,

- The infected populations send medical reports, which are collected by WBANs or any other sensors, to the cloud-hosting medical servers.
- Cloud service providers (CSP), either independently or collectively, conduct centralized medical data analytics.
- Clinicians or medical researchers query the medical records of interest for further analysis or studies.

It is well recognized that accurate patients tracking and prediction of disease propagation are long-standing challenges in medical research domain, especially due to the highly dynamic migration thanks to modern transportation. We envision that the proposed MCS-based disease control and prevention could offer a novel alternative to enable effective eHealth monitoring at a large scale, although some technical challenges must be tackled for particular implementations. Among the many foreseen advantages of MCS in eHealthcare early recognition of disease symptoms is the most important one, as it enables better control and understanding of diseases evolution, leading to more accurate intervention and ultimately achieving either timely treatment or propagation prevention.

III. Use Cases

In this section, we present a few examples of eHealth monitoring applications in our daily life. The proposed framework illustrated in Figure 1 can be always taken as a reference to understand our use cases.

3.1 Realtime alerts for monitoring heath condition

Assuming Alice is the user of our proposed eHealth monitoring system who has family history of heart disease. The doctor may suggest her to get a heart monitor sensor implanted into her arm. The sensor is powered by her body's own thermal energy and constantly monitors her heart rhythm and it is able to detect even the smallest arrhythmias (i.e. a condition under which the heart beats with an irregular or abnormal rhythm). In case of any alarming changes in heart rhythm, the sensor sends a text message to the patient's smartphone, saying: "This is your heart, Please rush to the nearest hospital immediately."

3.2 Chronic disease emergency

We assume that different patients and doctors are registered in a service provider's infrastructure which is located somewhere in the cloud datacenter. We also assume that different patients can be reached by 3G communication system and WiFi access points. Situational awareness IoT sensors send medical data via their personal servers periodically. If one patient suffering from a heart disease needs emergency evacuation to the hospital during his/her shopping, then we can imagine the following two scenarios: (1) Assuming that all sensors installed inside, on and around the patient body which monitor blood pressure, temperature, and heart beat etc., and send the readings to the cloud, and the (2), In this scenario, we assume that the patient can manually calculate readings of his heartbeat, blood pressure, temperature etc., through software sensor installed in his/her smart-phone and send them to the cloud. In both cases, upon receiving such alarming medical data of this particular patient, the service provider will immediately pass this data to a particular physician or specialist doctor and ambulance service center to

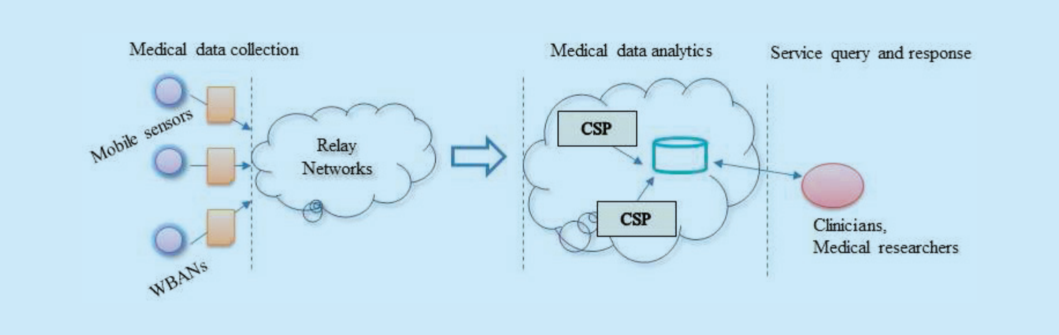

Fig.3 *Mobile Crowd Sensing for epidemic studies*

evacuate the patient to the hospital. Moreover, the service provider can communicate with the doctor or hospital staff through personal mobile phone to avoid further delay. Within very short time, the patient will receive emergency services and he/she will be shifted to the hospital. It should be noted that in this scenario, reports sent by the patient may contain his/her location information through GPS sensor of the smart phone (information about the location is compulsory for a patient who is at high risk of heart attack etc.).

3.3 Privacy preserving emergency care

Suppose Alice faces heart attack during her shopping in a market which is far from her home as well as from the hospital. Upon arrival of the first aid mobile unit, at first, emergency service person reads Alice’s implanted RFID tag to retrieve her personal and medical data from the already established WBAN network. Afterwards, various healthcare personals can directly access the measurements of her vital signs in real time manner. For instance, a nurse inquires on Alice’s health status from her WBAN and uploads an electronic report to the local server. Alice’s personal server or smart-phone which works as Personal Digital Assistant (PDA) is already configured with an initial Access Policy (AP) which can give access to her medical data. This predefined access policy will give a fine grained access to Alice’s medical data in this emergency case. It should be noted that the access policy in the emergency case should be lenient in order to provide the best medical services to the patient (Alice). Such predefined access policy do not give privileges to the medical staff to access medical data of the Alice other than related to the cardiovescular diseases. For example, her sensitive HIV record is only allowed to be accessed and shared with her particular specialist doctor. Therefore, medical team dealing heart related emergency of the Alice is not allowed to access her medical data of the HIV related diseases. Such type of access control can preserve the privacy of the sensitive medical data of the patients in eHealth monitoring systems. In eHealth monitoring systems, medical data is often stored and accessed distributively specially in case of the medical emergency. We further assume that Alice's predefined access control ensures security and privacy of her medical data during the heart attack. Since, Alice’s WBAN is constantly working to give fresh readings which are stored in the sensor nodes. As soon as Alice’s ambulance reaches in the wireless internet connectivity then Alice’s stored medical data is transmitted to the local servers in order to avoid wastage of the time by getting different vital signs readings before her extensive medical diagnosis.

IV. Performance Goals and Security Metrics

Balancing the tradeoff between performance goals and desirable security attributes is always an important issue for many ICT services. In order to understand the tension between them in the context of eHeathcare monitoring, one essential step is to specify the appropriate metrics for monitoring system utility and security.

4.1 Utility metrics

In [14], a set of metrics have been identified for evaluating safety and utility of implantable medical devices (IMDs), including data accessibility or availability, data accuracy, device identification, configurability, updatable software, multidevice coordination, auditable, and resource efficient. Despite the importance of those technical metrics in the design of IMDs, we firmly believe that the specifications of utility metrics should be derived from the practical needs of patients, clinicians, and other medical service providers, strictly complying with high-level requirements, regulatory, standards, and laws. In particular,

- From the perspective of clinicians, an eHealth monitoring system must provide sufficient and accurate medical information, aiding the clinicians in taking most appropriate medical treatment to the patients;
- From the point of view of patients, the monitoring system should run in extremely light-weight and unobtrusive way, collecting the only necessary and useful data that allow them to be accurately and timely treated.

Formally, we define the following utility metrics for eHealth monitoring systems,

- *Usability*. All the legitimate users involved in the monitoring process, especially patients and clinicians, should be very easily interact with the system and perform authorized operations, such as system initialization, configuration, software or firmware update.
- *Controllability*. Data collection at patient side should be fully under the consent of patients. One example is that a patient under continuous health monitoring should be granted the privilege to control what data can be collected and who has access to what data. The controllability can be delegated to the trusted third parties depending on particular applications.
- *Data quality*. The medical data collected from the patient should be accurate and reliable, providing sufficient information to clinicians for making correct treatments.
- *Dependability*. As a monitoring system is composed of heterogeneous functional units, their operations and interactions must strictly comply with control logic, keep working correctly in presence of *accidental* device errors or system faults such as device mis-configurations, communication channel interferences, software bugs.
- *Security*. The medical data collected from patients must be well protected from *intentional* attacks which may target at both hardware and software vulnerabilities.

4.2 Security metrics

As any other ICT services, eHealthcare monitoring systems must preserve confidentiality, integrity, and availability of patients' medical data, as well as their authenticity, accountability and non-repudiation in certain circumstances. In addition, privacy of patients should be sufficiently preserved according to the specific application scenarios and particular patient requests. For example, the authors of [32] have identified reliability, confidentiality, integrity, availability, and privacy as trustworthiness requirements of Personal Healthcare Systems (PHS). However, those coarse-grained security properties can be hardly quantified and evaluated without insightful understanding on the utility metrics of eHeath monitoring services, as discussed in Section IV-A. In [14], the authors have proposed a set of essential security and privacy requirements for IMDs, including authorization (personal authorization, role-based authorization, IMD selection), IMD device availability, device software and settings, device-specific privacy (including device-existence, device-type, device-ID), measurement and log privacy, bearer privacy (e.g., patient's name, medical history, or detailed diagnoses), and data integrity. Such a security analysis may present a valuable reference for assessing eHealth monitoring services in terms of desirable security metrics.

Revisiting the eHealth monitoring framework shown in Figure 1, we specify the security metrics as follows,

- *Patient-centric static privacy*. This may cover personal information such as gender, name, social security number, and so on. Those information are persistent and unique to a patient and can by no means be duplicated.
- *Patient-centric dynamic privacy*. This type of information may vary with patient's health status, including medical history, real-time collected medical data or physiological information, which are collected by IMDs and WBANs.
- *Patient-centric environmental privacy*. This type of information may contain geographic location and other IoT sensor data, which can be used to identify the patient's current situation.
- *Patient-device interactions*. This requires that patient relevant privacy should be well controlled and protected (three types of *privacy* specified above), while the data collected from devices should be well accessed and protected (*availability*, *integrity* and *confidentiality*).
- *Device-device communications*. This implies that the devices must be mutually authenticated (*authorization* and *authenticity*) in order to talk to each other via secure communication channel (*confidentiality*).
- *Beyond WBAN data delivery*. The data collected from IMDs and WBANs must be securely delivered to cloud service providers for further processing, primarily including computation and storage. A set of security requirements have been identified in [17], which falls out of the scope of our paper.

The given security metrics lay down an evaluation benchmark to evaluate the eHealthcare monitoring systems. Thus, given an eHealthcare monitoring system, it is imperative to conduct a gap analysis with the security metrics by identifying its security vulnerabilities. Considering the intrinsic complexity and heterogeneity of system components, the threat analysis should be conducted from a cross-layer perspective.

V. High-Level Security and Privacy Requirements

In order to develop effective security mechanisms to meet with those desirable security metrics, it is very important to understand the fundamental security and privacy requirements of eHealthcare monitoring systems. In particular, by taking into account the specific service context, we define *data security* as the data is securely stored and communicated to other entities/peers, and *data privacy* means that the data is accessed and used only by the authorized persons.

Regardless of the scenario-specific definitions, developing eHealth monitoring systems with sound security and privacy guarantees is one of the primary goals of all the stakeholders investing in healthcare domain. In the following, we will discuss the essential security and privacy requirements in healthcare systems, by classifying them into four main categories: administrative level security, network level Security, physical level security and information level security, as shown in Figure 4.

5.1 Administrative level security

As previously discussed, privileges granting policies and access control rules must be well defined, context-aware and adaptive to accommodate the required patients' health data availability and access flexibility properties, especially in emergency conditions.

- *Data Access Control*: data access control is a privacy preserving tool aiming to prevent any unauthorized access to the patient's personal and health data. In healthcare systems, the patient's medical data can be accessed by multiple stakeholders such as, doctors, nurses, researchers, health ministry as well as insurance companies\footnote{Usually, insurance companies can have very limited access, if not no access at all, to the patient's sensitive health information since they may refuse to issue/renew his/her insurance contract if they know that he/

she has a chronic or a critical disease for example etc.} etc., leading to an increasing risk of misusing such sensitive information. Therefore, role based access control model [17] is needed to enforce different access privileges for different participants. For example, doctors and nurses may have different access privileges to the patient's health record according to their responsibilities, while insurance companies might be allowed to access only the information related to the reimbursements of medical bills. Moreover, several access authorization levels should be granted to the doctors based on their role with regard to the patient's treatment; i.e. the doctor responsible for the patient's health status will have full access to his/her health information, while other doctors may have limited and adaptive access privileges depending on the context and circumstances.

- *Accountability*: applying the accountability mechanism [46] in eHealth monitoring systems aims to achieve more appropriate and efficient usage of the patient's health information by the legitimate users, and prevent any potential misuse that may threaten the patient privacy. Thus, by knowing that such mechanism is implemented by the system, any attempt to violate the granted access authorizations or to transfer the accessed data to an unwanted third party should be discouraged.
- *Revocability*: revocability consists in protecting a given system from compromised entities and users. If an entity or user is deemed to be malicious or compromised, then all the granted privileges should be immediately cancelled; e.g., in a Public Key Infrastructure (PKI) context, a certificate issued to a given user can be revoked if the certificate’s encryption keys are compromised or the encryption device is stolen. Therefore, the main purpose of the revocability mechanism is to prevent any harm that might be caused to the system as a consequence of the detected security breach (i.e. malicious behavior or compromised entity).

Moreover, administrative level security should cover robust and light-weight *authentication schemes* and regular audit of all involved administration entities. This will prevent eavesdroppers that pose one of the most significant threats to eHealthcare monitoring systems.

5.2 Network level security

The network security plays a major role in ensuring the security of the whole eHealth monitoring system since it provides safe transmission of the data from the sensing devices towards the remote data servers, and from these latter to the end user such as clinicians. Network security encompasses also securing the network devices against tampering attacks. In what follows we present the key security features that need to be ensured at this level.

- *Data Confidentiality*: data confidentiality means that the exchanged data through the network is properly protected from any type of man-in-the-middle attacks (MITM) which violate the data privacy and ultimately lead to the disclosure of personal health data to unwanted users. The components of the eHealth monitoring systems transmit very sensitive information about the patients who usually do not accept sharing it with others, as it reveals their health conditions (e.g. Diabetic, drug-addicted, early stage of pregnancy etc.). To protect the user’s privacy, all communications in healthcare systems should be encrypted. Data encryption in traditional sensors is usually achieved by encrypting the information before sending it, using a secret key shared on a secure communication channel established between the communicating entities. In case of inter device communications, the more appropriate way for encryption is the use of stream cipher algorithms, since in such algorithms the size of ciphertext is exactly the same as plaintext, and no extra data needs to be transmitted.
- *Non-repudiation*: non-repudiation property guarantees that the sender of a data cannot deny that he/she has not transmitted it. Simi-

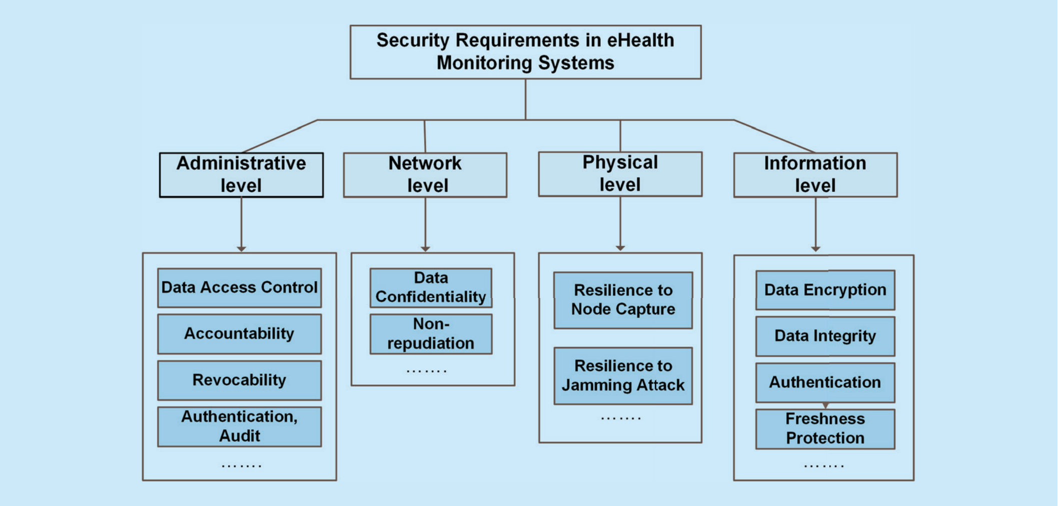

Fig.4 *Major security and privacy preservation requirements in eHealth Monitoring Systems*

larly, the receiver of this data cannot deny its reception from that particular sender. Generally, digital signature is the most widely used tool to ensure the non-repudiation.

5.3 Physical level security

Security efforts at physical level are devoted to the protection of eHealth monitoring system from threats targeting the physical sensor devices, in order to ensure the accuracy and trustworthiness of the data they generate. Hence, threats like sensor node capture and jamming attacks should be efficiently mitigated.

- *Resilience to Node Capture*: two main types of physical sensors can be distinguished in eHealth monitoring systems, namely, sensors placed on the patient's body, and the IoT sensors deployed in hospital premises or embedded in some equipment such as the hospital smart beds. The former type of sensors is responsible for measuring the patient's vital signs, while the latter measures the environmental conditions. Without robust physical level security mechanisms, attackers can easily capture a particular sensor node, retrieve its cryptographic keys and protocol state information, and finally clone it in order to redeploy multiple malicious sensors in the network. Such captured/compromised sensors can be placed into the eHealth monitoring system, leading to devastating impact on the whole system. This is a real challenge that requires a lot of attention from the research community to develop effective countermeasures [43].
- *Resilience to Jamming Attack*: although jamming attack has been extensively studied in the literature and several solutions have been designed to mitigate it, the specific characteristics of the environment in which the sensors are deployed in WBANs make it harder to detect and to deal with. In eHealth monitoring systems, WBAN sensors are often located within the transmission range of several IoT devices with varying power resources and processing capacities, which makes it easier for an attacker to target a given WBAN sensor and isolate it by jamming any data sent/destined from/to it.

5.4 Information security

Security of the information is the backbone of any eHealth monitoring system. Since eHealthcare applications involve not only medical recodes but also personal information, security and privacy preservation of such information are key concerns in this context. We outline below some key measures that can protect the data from various threats.

- *Data Encryption*: appropriate light-weight data encryption techniques can save data in transit from being exposed.

[1] Usually, insurance companies can have very limited access, if not no access at all, to the patient's sensitive health information since they may refuse to issue/renew his/her insurance contract if they know that he/she has a chronic or a critical disease for example etc.

- *Data Integrity*: another important factor of the security is the proper integrity check of the exchanged data to prevent any modification of its content while in transit.
- *Authentication*: appropriate authentication schemes can make data more secure, as it can prevent impersonation attacks.
- *Freshness Protection*: Replaying obsolete information is particularly harmful in eHealthcare context since it may lead to the spread of inaccurate or false readings about patient's vital signs, which in turn can mislead the clinicians in some critical decisions regarding this patient. Freshness protection is therefore imperative to prevent such attacks.

VI. Threat Analysis and Countermeasures: State of the Art

In eHealthcare monitoring system, there are various potential security threats that may significantly degrade the overall system performance and its trustworthiness level. In this section, we will limit our study to three major threat sources through which all other threat classes can be launched. These three sources are the patients themselves, insiders (i.e. authorized users and medical staff), and outsiders (i.e. unauthorized users), as described below.

- Identity threats: identity related threats can be launched using two different approaches. On the one hand, the patient may lose (or share) his/her identity information, enabling adversaries to get access to his/her eHealth account. On the other hand, insiders may use the patient identities to disclose a particular data of interest to a third party. This class of threats can result from one of the following scenarios: First, Loss of the identity, in which patients leave their login information on a public computer. Second, identity sharing whereby patients share passwords with outsiders (either intentionally or accidentally). Third, through social-engineering attack, causing passwords disclosure to outsiders. Last possible threat is insurance fraud, in this type of threat the insiders misuse patients' identities to get insurance reimbursement and obtain medical services.
- Access threats: (unauthorized access to eHealthcare data) in this type of access, the victim patient or any other legitimate user modification can give way to the unauthorized persons. This may happen due to the over-privileges granted to certain users. There could be any motive behind such act, for example, insurance fraud etc.
- Disclosure threats: unauthorized disclosure of medical data in eHealthcare system. Disclosure threats can be launched through any malware or file sharing tools and even by intentional or accidental password sharing.

It is well known that the eHealth monitoring system is vulnerable to several other threats mainly due to the inherited vulnerabilities from wireless networks. Indeed, the wireless channel, used as main communication support, is prone to various types of security attacks ranging from eavesdropping, data modification [39] and injection to jamming and Denial of Service (DoS) attacks [30]. Therefore, the security threats targeting this system can be also categorized according to the vulnerability that the attacker exploits to conduct the threat. First, threats as a consequence of the device compromise such as identity loss and, second, threats due to the network dynamics.

- Threats caused by device compromise: the tiny sensors used in the eHealth monitoring system are less tamper-resistant compared to other wireless devices and they can easily be compromised. Even if data stored in sensor node as well as on the local server is encrypted along with its encryption key, compromising the device will certainly lead to the disclosure of the data.
- Threats caused by the network dynamics: The eHealth monitoring systems are highly dynamic in nature due to their scalability from WBANs to the mobile crowd sensing. Due to the accidental failure or malicious activities, nodes can leave and join the network frequently. Moreover, some nodes may die due to the exhaustion of their battery power; therefore an attacker can launch attacks by masquerading authentic dead nodes.

6.1 Existing countermeasures

In this section, we present a detailed review of the existing solutions to the identified threats. We classify these solutions into two major classes: secure data storage related solutions, and data access related solutions.

Secure data storage related solutions: recently, Wang et al. [35], have used erasure coding technique to securely store medical data. Erasure coding is the method of data hiding in which data is first coded, then broken into segments and stored at several different locations. For example, original encrypted data is broken into *n* data blocks using erasure coding, where each data block contains its secret key. Then, those data blocks are distributed to *n* neighbor nodes for storage. All the sensor nodes, used for storing data, compute and broadcast an algebraic signature for each data block so that the integrity of the data can be verified. Signature size, computational and storage overhead of this scheme have been shown to be low. Consequently, this scheme can be considered as an appropriate countermeasure against data modification threats.

Fine-grained data access related solutions: in eHealth monitoring systems, it is necessary to establish fine grained distributed access control. Therefore, we will discuss below the existing schemes aiming to ensure the security of both the system and medical data.

- Symmetric Key Cryptography (SKC) based schemes: these schemes have proven an efficient way for distributed access control in eHealth monitoring systems. A solution proposed by Morchon et al.~\cite{morchon}, in which Blundo's key pre-distribution scheme is used to enable Role-Based Access Control (RBAC). Polynomial keys shares are pre-distributed, patients can easily establish pair wise key with any authorized entity and encrypt that particular data using this key. Mostly, SKC based schemes have few flaws with respect to their usage in eHealth monitoring systems, e.g., they have high key management complexity, and are vulnerable to users collusions.
- Public Key Cryptography (PKC) based schemes: Attribute Based Encryption (ABE) is one of the widely used techniques to ensure fine grained access control in sensor networks. ABE based scheme is one to many encryption method in which cipher text is readable to those group of users who satisfy certain access policy primitives. Such schemes are proven to be robust against collusive attacks, as in these schemes, colluding users are not allowed to derive any key belonging to the other users. Due to the expressive nature of its access privileges, this class of schemes seems to be promising solution for the fine grained access control in eHealth monitoring systems. In~\cite{Yusept2009}, the authors proposed Cipher text Policy ABE (CP-ABE) that perfectly addresses the needs of the role based access control. In this scheme, each user is assigned a set of attributes (roles), and the patients give permission to access their medical data to a particular set of roles/users. Finally, access privileges (AP) is built and which is used in the ciphertext. This scheme is based on tree-like access policy which is more expressive.

  As discussed in the Section V, accountability of the assigned access privileges is mandatory in order to avoid unauthorized access to the patients' medical data. In [48], Yu et al., have presented key abuse attack through accountability of the access privileges and proposed a solution that uses the revocability of the access privileges. To detect malicious activity of a pirate device, one frequently used technique is to trick the malicious/pirate device into decrypting tracing ciphertexts and If it succeeds in decrypting it, this means it will provide evidence of pirating [48]. Therefore, it is clear that for a honest (unsuspected) user, it is difficult to correctly decrypt a tracing ciphertext even if this latter contains its access control attributes. Yu et al. have proposed a broadcast based revocation scheme in WSNs [48], in which all the key updates are done through one broadcast message only.

- Anonymous Access Control and Authentication: Public Key Cryptography is still vulnerable to infer privacy information from the access policies. Therefore, some authors have used anonymous access control based schemes in order to safeguard eHealth monitoring systems from unauthorized accesses. For example, Zhang et al. [50] proposed an anonymous distributed access control scheme, which is based on the tokens issued by the healthcare center before accessing data in WBANs. In this scheme, blind signature is used to achieve anonymity. However, it is believed that this work has failed to achieve fine-grained access control because each anonymous user has the same access privileges. In addition, in [19], a pair of certificateless anonymous authentication protocols were proposed, allowing patients to access their medical data without any privacy leakage to the doctors or any third parties. However, a prior registration is usually required, making it inappropriate to emergency cases.

Based on the herein discussed access control schemes, we can conclude that Attribute Based Encryption (ABE) based schemes are more promising for achieving fine grained access control in eHealth monitoring systems.

6.2 A critical evaluation of the existing solutions

A security mechanism is the process of securing a given system from adversaries' attacks. It should have the capability to either prevent the attack, or detect it and trigger adequate reaction. This is a quite difficult task particularly for eHealthcare systems due to the limited processing power, storage, and communication capabilities of sensor nodes. Therefore, we will highlight the impact of such constraints on the efficiency of the above described solutions.

- Cryptographic based solutions: due to the above limitations of sensors, cryptographic techniques are not suitable for eHealthcare systems since they are either very expensive to implement or may significantly reduce the system efficiency. As eHealth monitoring systems carry sensitive information and deal with emergency situations, a failure to cope with efficiently with varying situations will certainly reduce the scope of the particular eHealthcare system. Therefore, the deployed cryptographic schemes should not affect the performance goals of the eHealth monitoring system. Some people argue that asymmetric crypto-systems are high-priced for medical sensors and interchangeable crypto systems do not seem to be versatile enough [40]. In general, there are three types of key management protocols, namely, trusty server, pre-distribution key management and self-imposing key management. Key management protocol is the basic step to construct any secure system. There are various types of the cryptographic keys which are setup and distributed to the nodes within the networks [41].
- Anomaly detection and response: Most of IDS and response schemes deployed in legacy computer networks cannot be applied to eHealth monitoring systems due to their heavy communication and computational overhead and operational complexity. Although the architecture proposed in [47] has potential to be applied as it addresses autonomic features of deployment environment, the design of particular anomaly detection engines, i.e., what features can be used to characterize anomalous events during monitoring process, remains to be non-trivial issue.
- Secure routing protocols: the routing function plays a major role in ensuring secure end-to-end data transmission in the network. However, due to the existing flaws in some routing protocols, WSNs and WBANs are exposed to several types of denial of service attacks, as outlined in [45].
- Trust and Reputation Management: trust establishment and management among the sensor nodes and the data aggregation nodes are essential for the proper functioning of eHealthcare systems. It is a bond of mutual association among all the devices of

the eHealth monitoring system. For example, a reputation management system like the one proposed in [34] can automatically isolate anomalous or malicious sensor nodes from the eHealth monitoring system, avoiding data to be polluted or manipulated. In order to enable the traceability of monitored objects and anonymity of the patients, the scheme proposed in [51] can be applied together.

- Secure Localization: providing proper location estimation of the patients is necessary in eHealth monitoring systems due to their relatively high mobility. Along with the different health related readings of the patients, medical sensors can also provide their locations. In [44], Boukerche et al., have described localization algorithms based on different geographical measurements, such as the distance, and angle estimation etc. The authors have also highlighted different attacks targeting patients' localization systems.

VII. Design Challenges: Dealing with the Tensions Between Utility and Security

Considering the objective of eHealth monitoring systems, a set of high level performance metrics can be specified for measuring the quality of performance goals. The major ones may include usability, cost-efficiency, dependability, accuracy, and security. This Section will discuss the design challenges associated with those desirable properties, primarily usability, security, and efficiency.

7.1 Usability: Patient-System interactions

It is well known that current eHealth systems lack of friendly interfaces for both medical staff and patients [18], which would be one of the major factors impeding their wider acceptance in practice. For example, most of existing healthcare systems require the patients to measure their own vital signs and send them to the data center, but those patients with chronic illness or in critical health conditions are unable to accomplish this task properly. Thus, the eHealth monitoring systems must provide highly automated equipment and tools, significantly reducing the user's involvement into the deployment, operation, and management. In addition, as patient-centric monitoring relies on the cooperation of multiple heterogeneous sensors, ranging from implantable or wearable sensors to smartphone and IoT sensors, their configurations must be transparent to the patients, avoiding any confusing or inconvenient settings. Despite non-trivial efforts from CHI (Computer-Human Interaction) research domain, the unique requirements on the design of user-friendly eHealth monitoring systems raise a set of challenges.

7.2 Cost-efficient and quality data collection

To obtain real-time, reliable and accurate health status of the monitored patients, the monitoring system must continuously collect the data of interest for a long period. This implies two requirements: first, medical data must be efficiently collected and updated, saving communication and computation overhead; second, the quality of data must be ensured, as the noisy or even false/inaccurate data may lead to wrong diagnose and further lead to human life risks. Clearly, there are tradeoffs between the two requirements. On the one hand, the cost resulting from data collection should be minimized, which however will impact the quality of data. On the other hand, in order to ensure the quality of data, the sensing coverage and duration must be maximized, which then will increase the cost and may affect the real-time availability of patients’ health status related data for medical staff.

To date, we have seen lots of efforts devoted to energy saving designs for Wireless Sensor Networks (WSN), ranging from communication protocol designs like MAC and routing to optimal sensor node deployments [1]. As a matter of fact, most of sensors, either WBANs or IoT sensors, are resource constrained and can hardly be rechargeable, especially implantable sensors, so the sensing algorithms and data collection methods must be extremely efficient. While due to the unique characteristics of WBANs, which usually relies on short range wireless communications and the sensors are well pre-distributed, most of energy efficient schemes for traditional WSNs cannot be directly applied to WBANs. This therefore calls for novel designs, ranging from power-saving sensor hardware [32], [24] and light-weight routing algorithms to optimal loading of applications [2].

Another challenge is that those employed sensors may collect and report false or noisy data due to unexpected hardware failures, unpredicted operating environmental factors, and unreliable communications issues. For example, as human bodies always keep moving and exposed to electromagnetic radiations, wireless communication would be error prone due to channel interference and signal fading, and routing paths may get unstable. In 1998, an experimental study has shown that low-power heart monitors at a hospital could be overwhelmed with electromagnetic interference, and become unable of providing critical care readings when a nearby TV station turns on a new digital television transmitter using a previously vacant TV channel [22]. Consequently, inaccurate or false data could be generated and collected, resulting in wrong diagnosis and even loss of lives if inappropriate medical intervention decisions were made. Meanwhile, as WBANs sensors operate in, on, or around human body, the negative consequences such as electromagnetic radiation and heats should be carefully considered as well.

7.3 Secure and privacy-preserving data processing

Despite the promising utilities of eHealth monitoring services, the patients would be reluctant to use them without convincing security and privacy guarantees. As aforementioned, the intrinsic vulnerable nature of sensor technologies and wireless communications allow malicious adversaries to gain overwhelming advantages to launch various attacks at patient side, and the attack targets could cover both hardware and software, ranging from heat emissions, radio signals and communication channels to different applications [25], [33].

First of all, data sensing and transmission may suffer from jamming attacks because of the open communications channels. For example, Gollakota et al. showed that it is possible to exploit the wireless connectivity between implantable medical devices (IMDs) so as to compromise the confidentiality of the transmitted data, finally leading to electric shock to the patient [12]. Similarly, the sophisticated might be capable of eavesdropping the communication links between near body sensors and personal servers or gateways, and even injecting forged data. For example, in [15] the authors reported several software radio-based attacks that could compromise safety and privacy of the patient wearing pacemakers and implantable cardia defibrillators (ICD). It is even not surprising to observe in the wild those attacks using simple power analysis or electromagnetic interference (EMI) to WBANs and other medical devices [16]. Furthermore, due to the co-existence of several WBANs in a small physical area, especially in hospitals, high interferences are inevitable and may lead to similar consequences as in the case of jamming attack. Therefore, accurately identifying the reasons behind the observed high interface (i.e. an attack or a normal situation) is a real challenge that deserves careful consideration.

Secondly, as medical sensors or devices need to run software for data collection and processing, the attackers may manage to break in the monitoring system by exploiting particular software vulnerabilities. In particular, Kevin Fu et al. pointed out that even old malware can be used to compromise medical device software [10], while malware tailed to WSNs and smartphones have been commonly seen in recent years due to the proliferation of mobile phone applications [29]. As eHealthcare monitoring systems rely on IoT sensors and smartphones to collect and relay the data especially for MCS based data collection shown in Figure 3, the infected software may open the door to attackers and further make the whole monitoring system compromised.

Last but not least, although we may assume that the patient data can be securely transmitted to remote data centers thanks to those sound security protocols like TLS, which unfortunately suffers from various attacks as well, the patients' data can still be comprised by attacks in the cloud and clinician side. These, however, are out of the scope of this paper, as we are more concerned with patient side data collection.

VIII. Multidisciplinary Approaches: Feasibility and Effectiveness

To tackle the identified challenges, the development of potential solutions must carefully balance the tradeoff between the performance metrics of concern in order to achieve the best quality of eHealthcare monitoring. In this Section, we will selectively and comparatively study a set of candidate approaches drawn from different research domains, with an objective to examine the feasibility and effectiveness of those existing schemes towards light-weight, reliable and secure eHealthcare monitoring services. As we are particularly interested in the tension between efficiency and security issues, our study will be conducted from two perspectives,

- How the design of security mechanisms can be tailored to eHealthcare monitoring systems by meeting with a majority, if not all, of performance metrics. Further, the introduction of security mechanisms should not lead to negative impacts on the performance goals.
- How the eHealthcare monitoring systems can be developed with built-in security and privacy mechanisms, or how the security and privacy by design approaches can be applied to develop eHealth monitoring systems.

8.1 Light-weight security mechanisms for eHealth monitoring

The previous analysis indicate that due to the intrinsic complexity and diversity of eHealth monitoring systems, the attack surface is extremely broad, meanwhile novel vulnerabilities and threats will be continuously introduced due to the dynamic nature. Thus, an in-depth defense line composed of diverse security mechanisms must be carefully leveraged to be integrated with eHealth monitoring systems in a light-weight and unobtrusive way. Here we will examine a number of available security mechanisms tailored to eHealth monitoring systems, which are intended to preserve *authenticity, confidentiality*, and *integrity* of medical data collected from patients.

1)*Collecting right data from right patient by right party*: As one of the major worries of patient is that some personal information is exposed, the monitoring process should strictly adopt *no more no less* principle. This implies that: first, the data can be only collected by the well authenticated parties; second, the data can be only collected when it is really needed; more importantly, the patient should be given a privilege to decide what data can be collected and who can collect that. This privilege is assumed if the patient health status allows him/her to make such a decision, whereas a default setting is used in case of emergency.

Making hardware device trustworthy. As an eHealth monitoring system is composed of numerous sensors and medical devices, all the involved systems must be trustworthy [9]. In fact, nowadays TPM (Trusted Platform Modules) has gained popularity for secure computation and communications of hardware devices, and its application to medical devices has been considered as well [13]. Another potential solution is Physical Unclonable Functions (PUFs) [21], which may enables a medical device to be efficiently and securely authenticated based on the unique hardware attributes. However, the generation of robust and perfect PUFs is still an open issue in the community. Regarding medical devices authentication, *one body authentication problem* was proposed in [6] for addressing the concern that the wireless sensors in a WBAN are collecting data about one individual and not several individuals. Despite the given solutions which are less efficient than TPMs or PUFs, more studies are desired.

Patient-centric authentication schemes. In order to preserve the privacy of patients, WBANs should be able to monitor the patients anonymously. As the solution, J. Liu et al. proposed a pair of certificateless remote anonymous authentication protocols [19], allowing patients to enjoy eHealth monitoring service while keep their identities unknown. However, in certain circumstances, some personal information such as geographical location, blood type, disease record must be known for better medical treatment. Upon the requests from medical staff, the patient should be given privilege determining to what extent his/her privacy information can be exposed. To address this issue, a patient self-controllable and multi-level authentication scheme was proposed in [20], which allows the patient to determine what type of data can be accessed by different physicians.

2)Ensuring medical data to be well protected: To protect medical data at rest or in transit, cryptography based techniques such as data encryption and cryptographic protocols are commonly used, which however may incur unwanted cost burdens for eHealth monitoring system. For example, the authors in [17] have discussed a set of cryptographic primitives for achieving secure medical data storage and access control, including SKC (Symmetric key Cryptography) and PKC (Public Key Cryptography) based schemes. Generally, such pubic key based schemes intend to protect the raw physiological information by encrypting them using public keys, which requires non-trivial computation and memory. Although symmetric cryptosystems theoretically consume less computational resource and communications overhead, the generation and management of keys must be sufficiently considered.

Alternatively, a straightforward yet efficient solution is to secure inter-WBAN communications and medical data transmission by exploiting the intrinsic characteristic of the human body [23]. We classify those schemes as *privacy by design* approaches, which will be discussed in the following Section.

8.2 Security or privacy by design

The ideal solution to simultaneously achieve efficiency and security is security or privacy by design approaches [4]. In another word, security and privacy must be taken into account from the scratch of data collection, avoiding any post-processing with the purpose of enhancing security or privacy.

1) Biometric cryptography for inter-WBAN communications: Although different WBAN sensors play different roles in data collection, e.g., optical sensors on the earlobe or toe for measuring pulse rate, sensor on the wrist for measuring blood pressure, electrodes on the chest for capturing electrocardiogram, microphone on the chest for capturing heart sounds, the physiological information can be generally represented as either electrocardiogram (ECG) or photoplethysmogram (PPG), which then can be used by biometric cryptosystems to generate the communication keys [23]. Compared with classic encryption schemes, biometric encryption has potential to improve security and reduce key management complexity [26]. However, one significant issue is to select the most appropriate biometric traits for generating the effective and robust keys [3], while the key agreement and management are also nontrivial [27].

Moreover, as WBANs usually use various frequency bands, especially some low frequency bands which have not been used in other similar wireless technologies. The propagation wave is then more likely to diffract around the human body rather than passing through it, and the path loss is higher when the sensors are placed at different sides of the body [7], [12], [18]. Therefore, leveraging these unique physical layer characteristics and combining them with the above biometric-based schemes will lead to significant improvement of security as well as keys generation and management.

2) Advanced signal and Image processing: As the physiological information is represented in signals and images, by carefully taking into account security and privacy concerns, the advanced signal and image processing techniques can be applied or improved for eHealth monitoring services. For example, compressive sensing has been widely recognized in signal processing domain as an efficient technique for data acquisition by exploiting the signal's sparseness. In particular, it has been successfully applied to biomedical image processing like MRI, as well as biomedical sensing applications [5]. By taking advantage of its intrinsic features, the authors of [28] showed that compressive sensing can serve as a core technique to achieve *privacy-aware* cloud-assisted healthcare monitoring system. Thus, we believe the recent advances of signal or image processing, together with novel sensor technologies and sensing paradigms, would significantly benefit to improving secure and efficient eHealth monitoring services.

IX. Conclusion

This paper surveys state-of-the-art approaches to designing efficient and secure eHealth monitoring. Specifically, we firstly presented a comprehensive framework for advanced eHealth monitoring system by describing, in detail, the entire monitoring life cycle. We have also highlighted the essential service components, with particular focus on data collection at patient side. To ensure high efficiency of the proposed framework, we have presented and analyzed the key challenges that need to be solved in order to develop efficient and secure patient-centric monitoring system. This concise survey paper is expected to serve as the blueprint for our future work based on a better understanding of the root causes leading to the inefficiency, if not failures, of existing security and privacy preservation schemes for eHealth monitoring.

Acknowledgments

This work was supported, in part, by Science Foundation Ireland grant 10/CE/I1855 to Lero - the Irish Software Engineering Research Centre (www.lero.ie).

References

[1] Z. Abrams, A. Goel, and S. Plotkin, "Set K-Cover Algorithms for Energy Efficient Monitoring in Wireless Sensor Networks," in Proc. of IPSN'04.

[2] Sawand M. Ajmal, S. Paris, Z. Zhang, and F. Nait-Abdesselam, "An Efficient Admission Control Algorithm for Virtual Sensor Networks," in Proc. of IEEE ICESS 2014.

[3] "The Practical Subtleties of Biometric Key Generation," in Proc. of USENIX Security 2008.

[4] A. Cavoukian, A. Mihailidis, and J. Boger, "Sensors and In-Home Collection of Health Data: A Privacy by Design Approach," Privacy by design Report 2009, Information and Privacy Commissioner, Ontario, Canada.

[5] F. Chen, A. Chandrakasan and V. Stojanovic, "A signal-agnostic compressed sensing acquisition system for wireless and implantable sensors," in Proc. of IEEE Custom Integrated Circuits Conference (CICC), pp. 1-4, 2010.

[6] C. Cornelius, and D. Kotz, "On usable authentication for wireless body area networks," in Proc. of USENIX HealthSec 2010, Washington, DC.

[7] T. Denning, K. Fu, and T. Kohno. "Absence makes the heart grow fonder: New directions for implantable medical device security," Proc. of the 3rd conference on Hot topics in security (HOTSEC'08), 2008.

[8] Garth V. Crosby et al. "Wireless Body Area Networks for Healthcare: A Survey," International Journal of Ad hoc, Sensor and Ubiquitous Computing (IJASUC), Vol.3, No.3, June 2012.

[9] K. Fu, "Trustworthy Medical Device Software," Institute of Medicine Workshop on Public Health Effectiveness of the FDA 510(k) Clearance Process.

[10] K. Fu, J. Blum, "Controlling for cybersecurity risks of medical device software," Communications of ACM 56(10): 35-37 (2013).

[11] R. Ganti, F. Ye, and H. Lei, "Mobile crowdsensing: current state and future challenges," IEEE Communications Magazine, vol.49, no.11, pp.32-39, Nov. 2011

[12] S. Gollakota et al., "They can hear your heartbeats: non-invasive security for implantable medical devices," in Proc. of ACM Sigcomm'11, Toronto, Canada.

[13] C. V. D. Graaf, "Keep Medical Devices Secure with Embedded Platforms that Support TPM 1.2," http://www.medicalelectronicsdesign.com/article/security-standards- tpm-12-security-module

[14] D. Halperin et al., "Security and Privacy for Implantable Medical Devices," IEEE Pervasive Computing, Vol. 7, No. 1, JanuaryMarch 2008, pp. 30-39.

[15] D. Halperin et al., "Pacemakers and Implantable Cardiac Debrillators: Software Radio Attacks and Zero-Power Defenses," in Proc. of IEEE Sym-

posium on Security and Privacy 2008.

[16] D. F. Kune et al., "Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors," in Proc. of IEEE Symposium on Security and Privacy 2013.

[17] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area network," IEEE Wireless Communications pp. 51-58, vol. 17, no. 1, 2010.

[18] X. Liang, M. Barua, L. Chen, et al., "Enabling pervasive healthcare through continuous remote health monitoring," IEEE Wireless Commu- nications, vol. 19, no. 6, 2012.

[19] J. Liu, Z. Zhang, X. Chen, "Certificateless Remote Anonymous Authen- tication Schemes for Wireless Body Area Networks," IEEE Trans. on Parallel and Distributed Systems, vol. 25, no. 2, pp.332-342, Feb. 2014.

[20] X. Lin, X. Dong, and Z. Cao, "PSMPA: Patient Self-controllable and Multi-level Privacy-preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System," IEEE Transactions on Parallel and Distributed Systems, to appear.

[21] R. Maes, "Physically Unclonable Functions: Constructions, Properties and Applications" Book, Springer, 2013.

[22] J. P. McClain, "Time to Upgrade. New telemetry standards call for a new generation of wireless equipment," http://www.ashe.org/resources/WMTS/pdfs/timetoupgrade.pdfv

[23] C. Y. Poon et al., "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," IEEE Communications Magazine, Vol. 44 Issue 4, pp. 73-81, 2006.

[24] M.-R. Ra et al., "Improving Energy Efficiency of Personal Sensing Applications with Heterogeneous Multi-Processors," in Proc. of ACM UbiComp'12, Pittsburgh, USA.

[25] M. Rushanan et al., "SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks," in IEEE IEEE Symposium on Security and Privacy, 2014.

[26] U. Uludag et al, "Biometric cryptosystems: issues and challenges," Proceedings of the IEEE, Vol. 92, Issue: 6, June 2004.

[27] K. K. Venkatasubramanian et al., "PSKA: Usable and Secure Key Agree- ment Scheme for Body Area Networks," IEEE Trans. on Info. Tech. in Biomedicine, Vol. 14, No. 1, 2010.

[28] C. Wang et al., "A Privacy-aware Cloud-assisted Healthcare Monitoring System via Compressive Sensing," in Proc. of IEEE INFOCOM 2014, pp. 2130-2138, Toronto, Canada.

[29] L. Wu et al., "The Impact of Vendor Customizations on Android Security," in Proc. of ACM CCS 2013, Berlin, Germany.

[30] S. Djahel et al. "Fast and Efficient Countermeasure for MAC Layer Misbehavior in MANETs," IEEE Wireless Commun. Letters 1(5): 540- 543 (2012)

[31] WBAN Standard, 802.15.6-2012 IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks.

[32] Y. Zhang et al., "Energy efficient design for body sensor nodes," J. Low Power Electron. Appl, 2011.

[33] M. Zhang et al., "Towards trustworthy medical devices and body area networks," in Proc. of the 50th Annual Design Automation Conference (DAC'13), Austin, TX, USA.

[34] Z. Zhang et al., "RADAR: A reputation-driven anomaly detection system for wireless mesh networks," ACM Wireless Networks, 16(8): 2221-2236, 2010.

[35] Q. Wang et al., Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance, Proc. IEEE INFOCOM 09, Apr. 2009.

[36] O. Morchon et al., Efficient Distributed Security for Wireless Medical Sensor Networks, Intl. Conf. Intelligent Sensors, Sensor Net., Info. Processing, Dec. 2008, pp. 24954.

[37] J. Bethencourt et al., Ciphertext- Policy Attribute-Based Encryption, Proc. IEEE Symp. Security and Privacy, May 2007.

[38] S. Djahel et al., "Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges," IEEE Communications Surveys and Tutorials 13(4): 658-672 (2011)

[39] S. Yu et al., Defending against Key Abuse Attacks in KP-ABE Enabled Broadcast Systems, SecureComm 2009, Sept. 2009.

[40] Le et al., "An Efficient Mutual Authentication and Access Control Scheme for Wireless Sensor Network in Healthcare" J. Networks 2011, 27, 355-364.

[41] Ng et al., "Security Issues of Wireless Sensor Networks in Healthcare Applications" BT Tech. J. 2006, 24, 138-144.

[42] Lorincz et al., "Sensor Networks for Emergency Response: Challenges and Opportunities" Pervas.Comput. 2004, 3, 16-23.

[43] Kavitha et al., "Security Vulnerabilities in Wireless Sensor Networks: A Survey" J. Inform. Assur. Secur. 2010, 5, 01-044.

[44] Boukerche et al., "A Secure Mobile Healthcare System Using Trust- Based Multicast Scheme," IEEE J. Select. Area. Commun. 2009, 27, 387-399.

[45] C. Karlof et al., "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures" In First IEEE International Workshop on Sensor Network Protocols and Applications, 2002, 113-127.

[46] D. J. Weitzner et al., "Information accountability" Communications of the ACM, 51(6), 82-87, 2008.

[47] Z. Zhang et al., "Toward cost-sensitive self-optimizing anomaly de- tection and response in autonomic networks," Computers & Security

30(6-7): 525-537 (2011)

[48] S. Yu et al., FDAC: Toward Finegrained Distributed Data Access Control in Wireless Sensor Networks, IEEE INFOCOM 09, Apr. 2009.

[49] A. Ramachandran et al., Computing Cryptographic Algorithms in Portable and Embedded Devices, IEEE PORTABLE'07, May 2007, pp.17.

[50] R. Zhang et al., DP2AC: Distributed Privacy-Preserving Access Control in Sensor Networks, in Proc. of IEEE INFOCOM'09, Apr. 2009.

[51] Z. Zhang, J. Liu, and Y. Kadobayashi, "STARS: A Simple and Efficient Scheme for Providing Transparent Traceability and Anonymity to Reputation Systems," in Proc. of DPM/SETOP, 2010: 170-187

Biographies

Sawand Muhammad Ajmal, is student of PhD in computer science in Laboratoire Paris Descartes (LIPADE) Paris Descartes University, Paris France. He did his Masters in Computer Science from University Jean Monnet Saint Etienne, France. He did his bachelor of engineering computer science from Mehran University of Engineering and Technology Jamshoro, Sindh Pakistan. Previously, he worked as Lecturer Information Technology in Sukkur Institute of Science and Technology (SiStech) Sukkur, Sindh Pakistan, from March 2006 to June 2009. His research interests cover Optimization, management and virtualization of sensor networks with current focus on privacy, security and energy efficiency of WBAN sensors.

Soufiene Djahel, received a Ph.D degree in computer science in December 2010 from LILLE 1 University-Science and Technology of France. During his Ph.D studies, he was working on security issues at MAC and routing layers in wireless multi-hop networks. Prior to that, he spent six months at INRIA NORD Europe research center as an Engineer Researcher. He received a Magister degree with majors in networking and distributed systems and a state engineering degree in computer science from Abderrahmane-Mira University (Bejaia, Algeria) and Badji-Mokhtar University (Annaba, Algeria) in February 2007 and June 2004, respectively. He is an Engineering Research Manager at University College Dublin (UCD) and a member of wireless networking group of PEL since February 2012. Before joining PEL, he was a postdoc fellow at ENSIIE where he was involved in a research project aiming at designing communication protocols for Hybrid Sensor and Vehicular Networks (HSVNs). His research interests include Intelligent Transportation Systems (ITS), security and QoS issues in wireless networks and Internet of Things (IoT). He is member of IEEE and a reviewer of its major conferences and journals in wireless networks and security. He was the general co-chair of VTM 2014 and the TPC co-chair of VTM 2012, and has served on the TPC of several conferences including IEEE ICC, IEEE WCNC, IEEE Globecom and IEEE IWCMC.

Zonghua Zhang, is an Associate Professor of Institute Mines-Telecom of France/TELECOM Lille. He is also an associate researcher with the lab UMR CNRS 5157 SAMOVAR. Previously, he worked as an expert researcher at the Information Security Research Center of NICT, Tokyo. He also spent two years as a postdoctoral researcher at the University of Waterloo, Canada and INRIA, France right after obtaining his Ph.D. degree from Japan Advanced Institute of Science and Technology (JAIST) in 2006. Zonghua has participated in a number of national projects sponsored by ANR (France), JSPS (Japan), NSERC (Canada), and NSFC (China), as well as some international collaboration projects such as NICT-Nano fund, France-Ireland PHC Ulysses project, FP7 EU-Japan collaborative project NECOMA. His research covers security management, anomaly detection, network forensics, and security protocols in various computer and communication networks, with current focus on security in Network Function Virtualization and Software Defined Networking. He has published over 50 papers in international journals and conferences, including ACM TAAS, IEEE TPDS, COMPSEC, IEEE DSN, ACM AsiaCCS, etc. He is on the editorial board of IEEE Communications Magazine and Intl. journal of Network Security. In addition to serving as guest editors in several journals, he has played different roles in organizing international conferences such as general chair, program chair, workshop chair, publicity chair, TPC members. He also serves as regular reviewer for prestigious journals and conferences like ACM TISSEC, IEEE TDSC, IEEE TIFS, COMPSEC, etc.

Farid Naït-Abdesselam, is a full professor of Computer Science at Paris Descartes University. His research interests include computer networks, security, sensor, ad hoc and vehicular networks, and healthcare systems. Farid Naït-Abdesselam earned his Engineering degree in Computer Science and Engineering from University of Algiers (USTHB) in 1993, and a Master of Science in Computer Science from Paris Descartes University in 1994. After 2 years spent in the industry, working as a software and network engineer, he started his doctoral studies in 1996 and received a PhD in Computer Science from the University of Versailles in 2000. He also holds the Habilitation à Diriger des Recherches from the University of Lille in 2009. He has published over 80 articles in journals and conference proceedings in his area of research.