Advanced Multi-parametric Monitoring and Analysis for Diagnosis and Optimal Management of Epilepsy and Related Brain Disorders: The ARMOR Project

Christos P. Antonopoulos[1], Nikolaos S. Voros[1], André Bideaux[2], Panagiota Anastasopoulou[2], Stefan Hey[2] and Wilhelm Stork[2]

[1] Technological Educational Institute of Western Greece, Computer and Informatics Engineering Department, Embedded System Design and Applications Lab, National Road Antiriou-Ioanninon, 30020, Antirio, Greece, 30020, Greece
{chantonopoulos, voros}@teimes.gr
[2] Karlsruhe Institute of Technology, Institute for Information Processing Technologies, Engesserstr. 5, 76131 Karlsruhe, Germany
{panagiota.anastasopoulou, andre.bideaux, stefan.hey, wilhelm.stork}@kit.edu

Abstract. The ARMOR project addresses the needs of the epileptic patient and healthcare professional, aiming at the design and development of a non-intrusive Personal Health System (PHS) for the monitoring and analysis of epilepsy-relevant multi-parametric data, (i.e. EEG, EOG, EMG, EKG, skin conductance data) and the documentation of the epilepsy related symptoms. ARMOR platform incorporates models derived from data analysis based on already existing state-of-the-art communication platform solutions emphasizing on security issues and required adaptations to meet ARMOR specifications. In this context, this chapter aims to provide an extensive description of the main aspects and issues addressed in the project as well as the main characteristics of the developed platform.

1 Introduction

In this chapter we are introducing the main concepts of ARMOR EU funded project. The main goal of the specific project is to manage and analyze a large number of already acquired and new multimodal and advanced technology data from brain and body activities of patients with epileptic disorders and controls (Magnetoencephalography (MEG), multichannel Electroencephalography (EEG), video, Electrocardiogram (ECG), Galvanic skin response (GSR), Electromyography (EMG), etc) aiming to design a more holistic, personalized, medically efficient and economical monitoring system.

The ARMOR project effectively tackles requirements posed by both patients and professionals, regarding a low cost yet highly efficient and secure ambulatory epilepsy monitoring platform. The platform is able to acquire as well as analyze (either

Hey S., Anastasopoulou P., Bideaux A., Stork W., Voros N. and Antonopoulos C.
Advanced Multi-parametric Monitoring and Analysis for Diagnosis and Optimal Management of Epilepsy and Related Brain Disorders: The ARMOR Project.
DOI: 10.5220/0006144500340055
In *European IST Projects - The Quest for Excellence Towards 2020 (EPS Vienna 2014)*, pages 34-55
ISBN: 978-989-758-101-4

online or offline) epilepsy-relevant multi-parametric data, (i.e. EEG, EOG, EMG, EKG, skin conductance data).

Epilepsy is a common, devastating and still incurable disorder. Although in most cases its symptoms can be ameliorated by life-long pharmaceutical treatment, still this treatment needs continuous adjustment and change to retain its efficacy. Due to its multifactorial causes and paroxysmal nature, epilepsy needs multi-parametric monitoring for purposes of accurate diagnosis, prediction, alerting and prevention, treatment follow-up and presurgical evaluation. The incidence of epilepsy is age-related, higher in children; epileptic seizures occur in 1-2% of the general population and in 4% of children. During the periods of childhood and adolescence non-epileptic paroxysmal events (NEPE) also occur more frequently than in adult life with similar clinical features. It is important to note that 30% of people with epilepsies have also NEPE. Furthermore, epileptic seizures differ with respect to motor, cognitive, affective and autonomic and EEG manifestations. Their recognition and full understanding is the basis for the optimal management (including additional diagnostic tests and genetics) and treatment. The total cost of epilepsy in EU is counted upwards of 15 billion euros per year, with the severe impact on the patient of the social stigma and the feeling of unpredictably seized, being unaccountable [1-3].

Current diagnostic methodologies and the need for advancement in this area comprise yet another important factor making epilepsy a prominent disorder to tackle. Such methodologies include video EEG that records the habitual suspected event or ambulatory EEG without video (for long term home recordings). Therefore, there is a need for more accurate diagnosis of integrated seizure phenotype in individual patients, which will allow better *understanding* of underlying mechanisms, *prediction (and alert)* of time and type of seizure (and alert) and availability of *medical assistance and advice* [4-9].

In order to tackle the aforementioned challenges, ARMOR project developed an ambulatory *monitoring* system for diagnosis and management, limited scalp EEG covering and custom-designed multi-polygraphy (textile based EMG, body activity sensors, autonomic and other biological data such as blood pressure, temperature, sugar blood levels and O_2 and CO_2 saturation continuous monitoring). Diagnosis of a disease as multifactorial and unpredictable as epilepsy demands continuous observation and correlation analysis of as many parameters as possible of the patient's brain, body and the environment.

In the context of ARMOR project, the above major medical problem has been addressed by employing the current advanced ICT technology and further advancement in data analysis included in a way, which will benefit both the patient and the economy of the health care system. In that respect, exploiting state-of-art wireless sensor networking technologies ARMOR is envisioned as an ambulatory monitoring system for diagnosis and management with video, limited scalp EEG covering and custom-designed multi-polygraphy (textile based EMG, body activity sensors, autonomic and other biological data such as blood pressure, temperature, sugar blood levels and O2 and CO2 saturation continuous monitoring). Therefore, issues such as efficient and robust communication performance, minimization of power consumption and integration of different diverse technologies comprise cornerstones of such endeavor. Furthermore, in the context of a complete end-to-end Personal Health System (PHS) ARMOR platform includes the development of information and Tele-alarm Server as well as client software for the ARMOR information and tele-alarm services. At the same time emphasis is paid on secure communication between client software, home gateway and wearable sensors while providing a wide range of health reporting services and applications (Mobile, web-based and in-the-cloud back-office). From the very beginning to the end of the project the theoretical background has also been elaborated and the effectiveness of the ARMOR sensors has been improved by targeted research work that proceeded in parallel with the steps described above. This research involved sophisticated analysis of existing data from expensive devices (that are not routinely available in clinics, e.g. multichannel EEG and/or MEG) and analysis of selected data obtained during ARMOR project, which represent prototypical examples or critical cases for diagnosis and classification.

2 System Architecture

Aiming towards a holistic, medically efficient and economical monitoring system ARMOR platform addresses all functional aspects required. Thus, following the overall system architecture as depicted in Figure 1 a critical segment comprises of the sensors enabling the data acquisition in the local site (e.g. the patient's home environment). Based on the extensive experience of ARMOR consortium as well as on the equipment provided by the involved partners, multi-parametric data acquisition is offered through a wide range of possible sensors gathering a wide range of medical data continuously and in real-time.

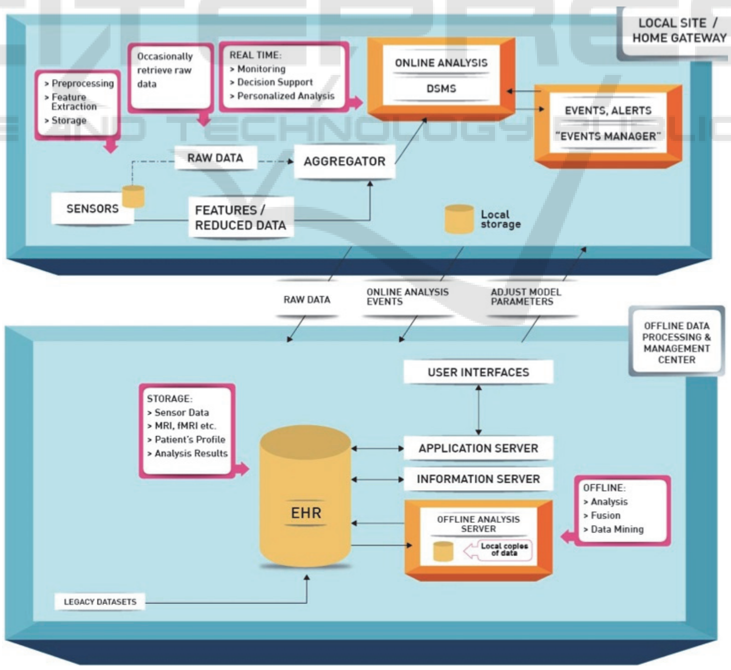

Fig. 1. ARMOR Platform Architecture.

The first level of data aggregation and processing is done at the home gateway where the ARMOR MiddleWare (AMW) provides access towards the upper modules and vice versa. The role of the AMW is crucial since it comprises of the gateway point between the sensor hardware equipment and the functional modules of software application. Specifically, on one hand, support is provided for all types of data and sensors utilized in the context of ARMOR, and on the other hand a wide range of services is provided in order to support the depicted functional modules. Furthermore, it functions as the communication bus among all required modules.

The ARMOR information server, as part of a complete remote Electronic Health Record (EHR) system, is also a critical component of ARMOR system since it hosts the models derived from extended research effort for multi-parametric data analysis. However, such functionality requires close collaboration with patient data stored in secure databases, which comprise another important subsystem of the ARMOR platform. Another functionally critical module depicted is the ARMOR Application Server. It provides to specialized personnel, like patients, medical stuff and caregivers, access to ARMOR system through a wide range of user interfaces. Such interfaces include visualization of multi-parametric data processing results, EHR access and personal tracking or nutrition habits and vital signs information.

Finally, ARMOR emphasizes on security issues of sensitive medical data through a specialized security layer where all ARMOR sub-systems area actively involved. The first layer tackling security issues are sensors ensuring secure data acquisition and transferring towards the aggregation point/s. All storage sites also employ security techniques ensuring data integrity and privacy. Data communication and data transferring are challenging issues that have to be addressed, especially when they are performed over the air. Both sensor communication and backhaul communication parts of systems like ARMOR are susceptible to a wide range of dangers and possible attacks requiring special attention. Finally, as far as the offline data processing and data management center are concerned, access rights, user authentication and authorization have also been taken into account as part of ARMOR EHR system.

2.1 Mobile Sensors for Multiparametric Monitoring in Patients with Epileptic Disorders

As ARMOR's main target is patients with epileptic disorders, it is vital to have EEG sensors present in the system, as it is an essential component in the evaluation of epilepsy. It has been shown that ambulatory long-term EEG recordings with intensive monitoring have led to better classifications of seizures and treatment results [10]. Because 30-60% of all patients are unaware of their seizures, multiparametric monitoring can lead to new results with optimal treatment. Without EEG recordings, false diagnosis may be made, as various phenomena are similar to the resulting behavior of a seizure.

Electrocardiogram (ECG) is used to record the electrical activity of the heart. It is an effective means to help to rule out a seizure being caused by the way the heart is working. It has been noted that in some seizures, especially those located in the temporal lobe, experience a change in heart rate prior to or at the onset of the seizure [11]. A study showed an increase in heart rate of at least 10 beats per minute in 73 %

of seizures (93 % of patients) and this occurred most often around seizure onset. In 23 % of seizures (49 % of patients) the rate increase preceded both the electrographic and the clinical onset [12]. Such changes may clarify the timing of seizure onset and can be useful for seizure diagnosis and for automatic seizure detection.

Therefore the goal is to develop a multiparametric monitoring system that assists in diagnosis, prognosis and treatment of the disease. Such system should fulfill the following criteria: it should be non-invasive, mobile, continuous and unobtrusive and all possible security and privacy aspects should be taken into account. This section describes the design of the sensors for mobile epilepsy monitoring.

2.1.1 Sensor Requirements for Multiparametric Monitoring of Patients with Epileptic Disorders

2.1.1.1 Functional Requirements

The functional requirement of ARMOR system include:

- *Sampling Rate:* The sampling rate for the physiological signals varies depending on the physiological parameter that is assessed and based on the state of the art research.
- *Resolution: The output of the sensors offers at least 12-bit resolution.*
- *Data Format:* The data format of the physiological sensor data that is used is based on the unisens-format. This is a universal and generic format suitable for recording and archiving sensor data from various recording systems and with various sampling frequencies.
- *Interfaces: The sensors communicate with the aggregator wirelessly by using the Bluetooth interface in order to transmit the pre-processed data for the online analysis or/and via USB in order to store the assessed raw data.*
- *Online Analysis:* The online analysis can be partially performed on the sensor side, where the data are pre-processed and on the aggregator where a novel Data Stream Management System (DSMS) effectively performs the further analysis that needs extra computation power.
- *Security:* The communication between the sensors platform and the aggregator employs encryption algorithms such as AES.

2.1.1.2 Non-functional Requirements

The non functional requirement of ARMOR system include:

- *Weight, Dimensions, Housing:* In order to develop a system appropriate for use in everyday life, the sensor platform have to be as unobtrusive as possible. Of course some technical limitations such as the battery consumption/ dimension might lead to bigger housings. A trade-off between the comfort and the system lifetime has to be made.
- *Usability:* Usability is a very important aspect that is also taken into account, as the end-users (Doctor, Patient, Healthcare Professional, Family Member or Caregiver) might be persons with limited technical knowledge. Therefore, the software

for starting/stopping the sensors offers an adequate GUI and special attention to user friendliness is paid.

- *Calibration & Service:* Calibration and service must also be supported by the producer/distributor of the specific unit.
- *Distribution to the End-users:* The patient will be wired-up at the hospital before he/she goes off to spend his/her day. The electrodes will be firmly fixed by the caregivers, whereas the sensors mostly needed for monitoring during nocturnal sleep will be easily placed / replaced by the patients before he/she goes to bed and unplugged in the morning after awakening.
- *Time of Use:* The sensors should be able to measure for at least 24 hours.
- *Price: The price of the final system will depend on the number of units that will have to be used.*

2.1.2 The ARMOR Sensor System for Mobile Epilepsy Monitoring

In order to achieve the main requirement, the multi-parametric monitoring, different sensors are integrated in the system. This includes not only the most relevant bio-signal for epilepsy monitoring, the EEG but also ECG, GSR and a push button that have be proven to be important in mobile epilepsy monitoring [13-15]. For this system the following sensors have been selected.

The EEG module (TrackitTM, Lifelines Ltd, Over Wallop, UK) is a mobile ambulatory device that can measure up to 32 channels with a sampling rate of 256 Hz. Each channel has an ADC resolution of 16 Bit and has a maximum differential AC input 10 mV. Depending on the number of channels, the sampling rate and the battery used the device can achieve up to 96 hours of recording.

The ECG module (ekgMove, movisens GmbH, Karlsruhe, Germany) is a single channel ECG recorder with a 12-bit resolution and a sampling rate from 256 Hz to 1024 Hz. The module can either be used with electrodes integrated into a wearable chest strap, which is light, small and comfortable or be used with conventional disposable wet electrodes. The electrodes of the chest strap are dry, allowing the everyday use. To assess the patient's physical activity, the module has also an integrated triaxial acceleration sensor (adxl345, Analog Devices Inc.) with a range of ±8 g and a sampling frequency of 64 Hz and an air pressure sensor (BMP085, Bosch GmbH) with a sampling frequency of 8 Hz and a resolution of 0.03 hPa.

Fig. 2. ECG-Sensor with activity monitoring module.

The GSR module (edaMove, movisens GmbH, Karlsruhe, Germany) measures the skin conductance with a sampling rate of 32Hz. The measurement range of the GSR module is

2µS to 100µS and its resolution is 14 bit. With this one can measure both the electrodermal activity level (EDL) and responses (EDR). Furthermore the module has the same sensor set to measure physical activity integrated as the ECG module.

Fig. 3. GSR Sensor.

The push button module (bioPLUX, PluX, Arruda dos Vinhos, Portugal) is a device that collects up to 8 signals from various sensors and transmits the signals via Bluetooth to a computer, where they can be viewed in real time. The resolution of bioPLUX is 12 bits, and its sampling frequency is up to 1 kHz. For this system only one channel with a push button sensor is used.

To assess additional context parameters like sound, light or geographic position, a smartphone can be used. Connection between Smartphone, Sensor and Aggregator is also realized by Bluetooth interface.

2.2 Communication Infrastructure

From communication point of view, ARMOR project developed a secure and efficient platform that is able to acquire data, aggregate them to a gateway on the home environment, exploiting state-of-the-art Wireless Sensor Network technologies and finally convey them to a data repository residing into a hospital or a caregiver facility. Consequently, a complete communication infrastructure comprises a multifaceted objective in order to achieve efficient and secure end-to-end data handling and transferring.

Respectively, the whole process can be segmented into three major parts: (a) the sensors data acquisition functionality, (b) the wireless transmission of data from the sensor to the aggregation point, and finally (c) EHR for controlling data management and data extraction from home gateway to the hospital facility.

2.2.1 Secure Sensors' Data Acquisition

Focusing on the sensors side, one key requirement is related to security. This is because respective devices comprise a potentially weak and vulnerable point in the whole chain of data flow. Specifically, typical WSN sensors employed in the ARMOR platform are small, low cost, devices operating unattended (e.g. in a patient's home environment) for extended periods of time thus being relatively easily acquired by unauthorized persons trying to access sensitive data. ARMOR sensors dispose of a Bluetooth interface, a debugger interface, a power supply and a local storage on a SD card. The debugger is used to read or flash the sensor and to debug the program. With respect to these main characteristics various alternatives have been studied and adopted to enhance security provision. To avoid the read of the data or the program code from the microcontroller, the debugger interface is disabled. The sensor platform disposes of a special interface to update the flash with a program code: the so-called "bootloader". This interface gives no access to the storage and can only be used to transfer a program. In the case of using an encryption of the local storage it is advisable that this interface is disabled as well. Additionally, attacks over the power supply are normally made in laboratory to get a secret key that is not changing and need to use measurement instruments direct on the sensor. In the case of a platform using data encryption, the secret key is changing periodically with respect to new measurements. The secret key is needed while saving the data on the local storage and so the user of the sensor will notice this kind of attacks.

ARMOR sensors are based on the MSP 430 microcontroller unit from Texas Instruments offering a performance optimized software implementation of the Advanced Encryption Standard (AES). This implementation is designed for the 16-bit RISC architecture of the Texas Instruments MSP 430 controller family and it is provide as a C interface offering high level security AES crypto features [16].

Research on similar commercial products has shown that no encryption mechanism on the local storage is used [17,18]. Based on the above risk analysis encryption on the local storage is not required.

2.2.2 Wireless Sensor Network Data Transmission

In the context of a demanding medical application, such as epilepsy monitoring, a wide range of different signals leading to diverse data traffic requirements are required to be transferred. For example, in ARMOR project the sampling frequency of signals acquired could span from few Hz or tens of Hz (e.g. accelerometer and respiration sensor) up to hundreds of Hz or around 1 KHz (e.g. EEG and ECG signals). Taking into consideration that each sample is typically represented by a 16-bit number as well as that in many cases multiple sensors are required in each case (e.g. a complete EEG monitoring may require tens of EEG electrodes) it can be easily deduced that a wide range of traffic rates must be supported.

However, selecting an appropriate technology is not straightforward due to the specific requirements posed by typical WSN sensors and platforms. During the last few years, state of the art WSN technologies exhibit impressive advances advocating respective system as a prominent solution for demanding applications. On one hand, advances in hardware design, integrated embedded systems and miniaturization have proven that extremely small devices, yet sufficiently powerful, can be implemented. Additionally, such devices offer the capabilities to acquire data from the physical world, store and process them, but even more importantly to transmit them wirelessly using embedded transceivers. On the other hand, software developments have introduced a completely new communication paradigm attracting high interest both from academia and industry offering flexibility, rapid network deployment, selforganization, distributed operation, power aware functionalities etc. All these capabilities offered have led to significant advancements in various networking areas especially focusing on physical, MAC and routing layers of the ISO/OSI networking model [17, 18] characterizing respective technologies.

However, offering the aforementioned characteristics comes at the cost of extreme limitations in critical aspects, which comprise Achilles' hill especially regarding processing power, storage capabilities, communication bandwidth and most importantly energy availability. The implementation of a typical WSN node is based on components with extremely limited resources such as low processing capabilities (usually provided by 16-Bit based Micro Controller Units), limited available memory (in the area of 10 Kbyte RAM) and scarce energy availability; most prominent WSN platforms base their operation on few AA batteries or even batteries with significantly less capacity like Shimmer [19] platform that uses 450 mAh batteries. At the same time, nodes are expected to operate unattended for extended periods of time.

Furthermore, in order to live up to the expectations of sensitive applications such as the medical ones, another equally critical aspect that short range wireless communication technologies have to address is the provision of adequate security. It is commonly accepted that in sensitive nowadays applications it is of paramount importance to guarantee that data gathered, stored and transferred comply with strict ethical and legislative regulations as well as data privacy, data integrity and authentication of communication parties [20]. In order to provide these features, we must rely on the efficient execution of robust and state of the art cipher algorithms. In the context of the ARMOR platform, Bluetooth protocol was employed for ARMOR WSN infrastructure, while IEEE 802.15.4 was also considered and evaluated.

Bluetooth is a wireless radio specification designed to replace cables as the medium for data and voice signals between electronic devices. The specification is defined by the Bluetooth Special Interest Group (SIG), which is made up of over 1000 electronics manufacturers. Primarily intended for mobile devices, Bluetooth's design places high priority on small size, low power consumption and low costs. Bluetooth specification seeks to simplify communication between electronic devices by automating the connection process.

Bluetooth radios operate in the unlicensed 2.4 GHz Industrial, Scientific, and Medical application (ISM) frequency range. This frequency is already widely used by all kind of devices such as microwave ovens, baby monitors, cordless telephones, and 802.11b/g wireless networking devices. In order to avoid interference from these devices, Bluetooth uses a technology called *spread spectrum frequency hopping*. Spread spectrum frequency hopping changes the transmission frequency up to 1600 times per second across 79 different frequencies. As a result, interference on any of those frequencies will only last a fraction of a second. This, coupled with the limited range of Bluetooth radio transmitters, results in a robust signal that is highly tolerant of other devices sharing the same frequency.

Contrary to IEEE 802.15.4 based solutions, where all relative platforms are characterized by analogous capabilities, Bluetooth based solutions vary significantly depending both on the version of the protocol supported and even more on the specific implementation's characteristics. Therefore, concerning data rates solutions covering a wide range from 300 Kbps up to 1.5 Mbps can be found [19], [21], [22].

Furthermore, contrary to IEEE 802.15.4, which effectively leaves security support to the higher ISO/OSI layer, Bluetooth offers a complete security specification with respective advantages and disadvantages. Bluetooth security is based on three critical services: *authentication*, *authorization*, and *encryption*. The authentication service is supported by ensuring that a device seeking a connection is indeed the one it claims to be. Authorization is the process that determines whether or not a requesting device is allowed access to specific information or services. Encryption helps to ensure confidentiality by protecting private data from being viewed by unintended recipients.

Bluetooth v2 devices, upon which ARMOR platform is based, can be set in one of three different security modes. In security mode 1, no security measures are utilized. Any other Bluetooth device can access the data and services of a device in security mode 1. Security mode 2 enacts security measures based on authorization. In this mode, different trust levels can be defined for each of the services offered by the device. Security mode 3 requires both authentication and encryption. The security features of the Bluetooth specification provide for secure communication at the link level that comprises a weak point. Moreover, there are some weaknesses that need to be considered. These weaknesses arise from the specification's heavy reliance on device authentication for security services as well as the level of control that the user has over Bluetooth devices and their configuration. The current Bluetooth specification does not provide any means of user authentication. The lack of any means of user authentication coupled with the reliance on device authentication leaves Bluetooth particularly vulnerable to spoofing attacks and the misuse of authenticated devices [23].

Based on projections indicating the rapid increase of short range wireless communication devices (e.g. in the context of a cyber physical system) the need for more secure systems using stronger cipher algorithms, while not requiring excessive resources, will also increase. Even more, provision should be made for cases where new communication technologies will appear or when existing technologies (e.g. Bluetooth) will need to coexist with new ones without compromising security level. In such cases, an implementation not being limited by cipher algorithms of particular communication protocol (e.g. E0 and E1 of Bluetooth) but rather following a more widely adopted paradigm (e.g. AES) will be of significant added value.

In order to deal with the aforementioned challenges, in the context of ARMOR an ultra-low power hardware encryption module has been developed. It provides high security level regardless of the underlying communication technology employed and is based AES encryption algorithm [49]. AES algorithm has been standardized by the National Institute of Standards and Technology (NIST) as a highly secure block ciphering method. It has replaced the old DES algorithm, whose key sizes were becoming too small. The developed encryption module implements AES algorithm in FPGA technology and is highly optimized for ultra-low power dissipation rendering it an ideal solution for WSN network applications. The encryption module has been carefully designed to require minimum logic resources as well as utilizing power aware design techniques in architectural (8-bit datapath, use of sequential structures, resource reuse, optimized Galois Field Multiplier which is the structural datapath element of the cryptographic engine, pipelining, path balancing, one hot FSM encoding) as well as in FPGA implementation level (clock and data disabling). The use of these techniques has resulted in a significant performance/silicon footprint ratio [24].

2.2.3 Personal/Electronic Health Record Technologies

In the context of a holistic approach like the one offered by ARMOR project, the adoption of the proper EHR technology is of paramount importance. As part of ARMOR system it entails all aspects of data handling, management and transferring from the home environment of the user (i.e. the patient) to the service provider that can be a hospital, a clinic, a doctor or any kind of care giving facility. ARMOR's Personal Health Records (PHR) intends to be a standard electronic management system of medical information exchanged on between the patient and his/her physicians, as well as amongst medical organizations that collaborate for providing integrated medical care services. ARMOR PHR has been designed using the latest technology that allows efficient and secure handling of patients' sensitive medical data.

Significant effort has been devoted to security aspects since in today's global and mobile economy, it is common to hear stories of companies paying significant costs and exposing themselves to lawsuits due to corporate assets and data being compromised. At the same time, IT departments started to face new risks associated with the growing need to support remote access to mobile users, partners and customers. Administrators must constantly compromise the risks associated with providing remote access with increasing demands for mobility. Remote users require access to company's resources any time from anywhere, using any computer whether it is provided by a company, own laptop or an internet cafe PC, mobile or handheld PDA device. E-Health systems, platforms and services are also examples of such requirements. They employ standard networking technologies and hence they are vulnerable to same types of attacks. Having to deal with extremely sensitive private and personal data, they are also exposed at the risk of law suits and they need to employ much more stringent security mechanisms, including data acquisition from distributed medical instruments and protection of (often) distributed EHR repositories against intrusion and data theft.

The end-to-end security is one of the possible approaches to counter fight these risks. End-to-end security means that sensitive data are encrypted all the way from the device side application back to the enterprise. Rather than relying on transport-level security (such as Secure Sockets Layer, or SSL), end-to-end security puts the power of strong encryption in the user's hands, all through a simple interface. The specific requirements posed for the technology adopted in ARMOR included: authenticated and authorized sensor information access, secure Web service interfaces to PHR and secure Web services with HTTP.

Nowadays the area of EHR technologies has attracted high interest as indicated by the wide range of standardization bodies involved [25]. The data structure algorithms and the user iInterfaces proposed [26-28] as well as the number of different and diverse implementations [29-33]. The ARMOR platform has adopted the intLIFEPHR solution provided by Intracom S. A. Telecom Solutions, which is member of the ARMOR consortium. intLIFEPHR consists of the following subsystems:

- Electronic Health Record Subsystem
- Vital Signs Monitoring Subsystem
- Personal Health Record Subsystem
- intLIFE Management Subsystem

Through the above features intLIFEPHR perfectly suited the needs of the ARMOR platform offering an efficient, robust and secure backhaul connection between the home environment and caregivers' facility.

2.3 System Middleware

The ARMOR Middleware (AMW) represents the ICT component that provides the necessary infrastructure to acquire & store locally and upload to remote server (the PHR) sensor data. It provides infrastructure for real time computation of raw sensor data (modalities) along with the necessary data aggregation and synchronization functions. It also provides a notification module that communicates specific events (mainly alarms) to high-level applications

AMW consists mainly of three parts. The first part is the xAffect that collects all the data from the sensors and fuses them to a synchronized data stream. The second part is the graphical user interface. It is used to interact with the patient or healthcare professional and also handles the data storage and uploads. The last part is the Data Stream Management System (DSMS), which it uses the data stream to perform online analysis to detect events of special interest.

2.3.1 xAffect

xAffect is a software framework developed by the Research Center for Information Technology, Karlsruhe, Germany. It has been developed in Java to fulfill real-time data processing, easy integration of different data sources, easy integration of algorithms and data logging of raw as well as derived data [34]. The data format, which is being used, is the unisens-format. This is a universal and generic format suitable for recording and archiving sensor data from various recording systems and with various sampling frequencies [35].

Although xAffect™ offers much functionality, in the context of ARMOR two main parts of it have been tailored to ARMOR needs: *data streaming* and *data recording*, which fulfill AMW's integration requirements successfully. However the capabilities for data fusion remain available as complement to the data stream management system, named ARMOR Insight.

Version 1.01.846 of xAffect™ allows to use it as library, which resulted in embedding it as a component in AMW. The specific version has also been modified in order to customize the interface with AMW that was necessary to achieve the performance and the functionality required for the AMW. The changes that were introduced can be summarized as follows:

- Additional libraries for bioPlux and TrackIT. In order to use a broad spectrum of sensors, non-existing libraries had to be written from scratch.
- A decryption module that allows realizing ciphered data coming from ARMOR sensors will come ciphered.
- Data acquisition pause/resume to achieve the needs for the control of the sensor data acquisition.
- A custom notification module for communicating xAffect state to AMW DSMS.
- Data recording functionalities have been extended to provide configurable file

splitting (in order to reduce high network consumption during heavy data uploads), alarm signal detection and a communication system with AMW PHR up loader daemon.

- Data streaming functionalities have been extended to provide hot-plug client connections and custom xml output data formats (including gzip for network traffic optimization).

2.3.2 Graphical User Interface

In the Graphical User Interface (GUI) the user enters his/her username and password and the patient-id, which corresponds to a personalized profile from the Server. Afterwards the user can press the configure button to initialize the communication with the sensors. Furthermore the profile contains information about the alarm settings. This enables the system Middleware to set up the DSMS with the customized set of alarms [36].

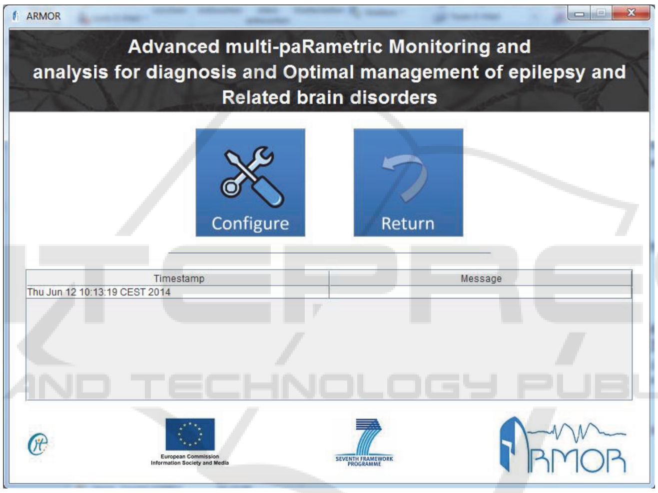

Fig. 4. ARMOR Graphical User Interface.

When the configuration process has finished successfully the user is able to start the measurement by pressing the record button. During recording, the data are streamed from the sensors through xAffect towards the DSMS and the local storage. The GUI also allows the user to pause or resume the measurement. This allows the subject to interrupt the data acquisition and move out of the Bluetooth range of the Home Gateway.

2.3.3 Data Stream Management System (DSMS)

The DSMS function takes place on-line, where real time processing of modalities is performed. The DSMS is based on Microsoft™ StreamInsight™ platform created for the development and deployment of complex event processing (CEP) applications.

It's a high-throughput stream processing architecture that uses .NET Framework-based development platform.

The development done at the DSMS allows receiving xAffect™ sensor data in real time and forewards them in a lossless way to the computation algorithms. In this way, the framework is able to create queries and policies over data.

Lossless data streaming between xAffect™ and DSMS is achieved by employing TCP channel. This makes sure the built-in architecture of StreamInsight™ can work with the synchronized data coming from xAffect™.

The main objective of the DSMS is to deliver alarm and warning events predefined in the profile. One of the most important events is the push button detection. Other events are for example an alpha rhythm or seizure detection.

3 Epilepsy Monitoring and Data Analysis

The proposed system provides novel functionality for both real-time (online) and offline analysis of data. New techniques have been developed for multi-parametric sensor data mining (data fusion and correlation analysis, integration of information from various data sources/modalities, similarity analysis of signals, clustering, classification and prediction). Novel real time (online) analysis methods for multi-parametric stream data have also been developed aiming at detecting signals beyond the limits, identify seizure premonitory signs, discover typical patterns of activity followed by seizures and detect any typical patterns of activity/behaviour based on models that will be created. Trade-offs for automated analysis are taking place at the local site of each patient (instead of at the Health Center) aiming to reduce processing time, storage requirements and communication cost, facilitating the reduction of raw data to secondary and tertiary parameters (that have been correlated), have also been taken into account. All analysis and emergency alert mechanisms are based on a personalized model according to the patient's health profile. New decision support tools for advising the patient, triggering an alarm and detecting emergency situations have also been developed.

In addition, new informatics tools have been developed for offline analysis of multi-parametric data correlation with other stored data about the patient (EEG, PET, SPECT, fMRI, genetic data) and the disease, offline data fusion for certain combinations of modalities (e.g. MEG, MRI) taking place at the Health Center with the participation of medical experts as well as new functionality that will provide feedback to the online analysis model. ARMOR has also contributed with novel contributions in the analysis of multidimensional time series, similarity analysis of signals, detection of patterns and associations between external indicators and mental states, analysis of associations among signals and symptoms, discovery of lag correlation among different signals, detection of vital signs of a person changing in a significant manner, identification of motifs (in spatio-temporal signals) and frequently repeated patterns or outliers (corresponding to seizure signs), and automatic summarization of results for each patient.

Moreover, new techniques have been investigated for the detailed offline tomographic analysis of multichannel EEG and MEG data recorded simultaneously with measurements of heart activity (EKG), Galvanic skin Response (GSR) and other measurements that can be easily incorporated in the online monitoring for normal and epileptic patients in awake state and at different sleep stages obtaining the most direct insight of what is happening in the brain. As far as sensor data acquisition and pre-processing (cleaning, integration, transformation and reduction) are concerned, both existing and novel techniques for data reduction and summarization (to deal with data streaming) have been considered.

Finally, in the context of ARMOR, existing database technologies have been extended to support the organization of multi-parametric data including the support of efficient storage and retrieval capabilities such as multidimensional indexing. The ARMOR databases store logs of all events, recorded values from sensors and other metrics that are monitored, personalized patient health profiles, medical information including guidelines for diseases, symptoms, medication, potential side effects of medication, etc.

3.1 Current Practices and Challenges for Epilpsy Monitoring

Unprovoked seizures and epilepsy are fairly common treatable neurological conditions (incidence of unprovoked seizures 33 to 98 per 100,000 per year; incidence of epilepsy 23 to 190 per 100,000 per year; prevalence of epilepsy 3 to 41 per 1000; lifetime risk of epilepsy: 1 to 3%) [37]. There is considerable disagreement about the recurrence risk following a first seizure. Estimates of the recurrence rates following the first seizure over two and three years have varied between 23% [38] and 71% [39]; the risk of recurrence has been estimated at 14% at one year, 29% at three years and 34% at five years [40]. In a systematic review and meta-analysis including both prospective and retrospective observational studies, the pooled estimate of the risk of recurrence of a first unprovoked seizure at two years was 42% (95% CI 39 to 44) [41]. The more seizures an individual have had, the higher the risk of subsequent seizures; the risk of a recurrence following two seizures is approximately 73% and after three seizures is 76%. There is evidence that early treatment can reduce the risk of seizure recurrence, and its efficacy depends largely on the appropriate drug choice in relation to the particular clinical syndrome. Therefore, early and accurate diagnosis of epilepsy is crucial in patients' management. However, there are two important clinical problems to consider.

First, the initial symptom of epilepsy (the first seizure in life) usually manifests as an episode of loss or impairment of consciousness, usually associated with change of muscle tone. The diagnostic challenge here is to distinguish an epileptic seizure from other medical conditions that present with similar clinical features but require completely different and specific for each clinical category treatment and management. These clinical entities manifest as non-traumatic transient loss of consciousness, i.e. a brief clinical episode, characterised by rapid loss of normal responsiveness, loss or reduction of muscle tone or stiffness and amnesia for the event [42].

Second, the generic term "epilepsy" is unsatisfactory for clinical use. Intense clinical and genetic research over the last few decades have identified a large number of well defined epilepsy syndromes with different clinical, EEG, neuropsychological, and neuroimaging profiles, natural history and prognosis, conditions that ultimately require different management. Identification of the particular form or epilepsy syndrome is the cornerstone of meaningful, optimal management.

Therefore, there are two major steps in the orderly diagnostic process of the patient with possible new onset epilepsy: 1) is it epilepsy or another disorder of Transient Loss of Consciousness (TLC)? and 2) what type of epilepsy is it?

Syncope is the commonest cause of TLC, due to cerebral hypoperfusion. *Neurally mediated* (vasovagal, neurocardiogenic or reflex) syncope can happen in up to 40% of the general population and can be misdiagnosed as epilepsy, particularly when it results to cerebral hypoxia and to a *reflex anoxic seizure*. *Cardiogenic* syncope is due to structural heart disease or arrhythmia, and *psychogenic syncope* can mimic organic types of syncope [43].

Detailed history regarding possible triggers and the circumstances of the event and accounts of several episodes from patients and onlookers are essential for the diagnosis of syncope and its differentiation from epilepsy and other causes of TLC. Physical (heart auscultation and BP measurements) and neurological examination may reveal specific cardiac or autonomic disorders and prompt the relevant referrals. An EEG is not a basic ancillary test, unless a diagnosis of epilepsy is likely; however, on rare but well documented occasions, focal epileptic seizures (mainly right temporal) may trigger cardiac asystole and anoxic seizures. Important laboratory tests include:

- Electrocariogram (ECG) which determines the cause in less than 5% of cases [44].
- Echocardiography, of undetermined but generally small diagnostic yield (detects structural cardiac abnormalities) [45].
- Exercise test, of less than 1% diagnostic yield. Prolonged monitoring for 48h (Holter) or few weeks (continuous loop recorders) or months (invasive Medronic device planted subcutaneously). A frequent problem is detection of arrhythmias without symptoms.
- Tilt table test (positive in 50% of patients with syncope) [46].
- Other autonomic function test (of undetermined but generally small diagnostic yield, time consuming and expensive).

Diagnosis of epilepsy may also require differentiation from other paroxysmal events that may alter or appear to alter neurological function to produce motor signs or sensory, autonomic or psychic symptoms that at least superficially resemble those occurring during epileptic seizures. Such clinical events are typically known as *non-epileptic seizures* (NES), and can be either of physiological (PhNES) or psychogenic (PsNES) origin; distinction between these two types is important for proper treatment and management and relies on recognition of organic symptoms and signs. More than 30% of the patients referred to epilepsy centers have NES only whereas a smaller proportion has epileptic and NES in combination, particularly PsNES.

In order to deal with the aforementioned challenges, ARMOR allows progress beyond the above diagnostic and follow-up procedures by:

- Combining all appropriate measurements of brain and body activity at the same time.
- Integrating these multi-parametric and multimodal data so as to allow better differential diagnosis of epileptic from non-epileptic seizures as well as to define better the type of epilepsy seizures represent.

- Allowing a custom made selection of the most simple and economical sensors to be employed in each patient, based on (a) advanced analysis of data with initial extended use of many sensors and (b) experience gained from advanced analysis of similar cases.
- Allowing the final monitoring to be conducted at the patient's (child's) own physical environment and in a cheaper and more efficient way (for clinical purposes).
- ARMOR also provides a valuable clinical tool to clinical epileptologists as it solves several different current technical problems of long term monitoring and communication of the many parameters needed to describe the complex nature of paroxysmal seizures.
- ARMOR through basic and clinical research has shed light to our ignorance on several questions of epileptology which demand long term and accurate multimodal and multi-parametric monitoring including: (a) electroclinical correlations of loss of consciousness in generalized seizures, (b) sleep/epilepsy relationships and (c) stress and other triggers/premonitory signs of epileptic seizures.
- The possible relationship of above to the localization of epileptic foci activations in brain space - with implications to pathophysiology of epilepsy and its therapeutics including presurgical evaluation.

3.2 Offline Data Analysis Algorithms

The offline data analysis in ARMOR has two main goals: to help accurate diagnoses and to support the online monitoring of patients. Various methods have been developed. These newly developed and other, already available, methods have been used to analyze data from patients with epileptic disorders and healthy individuals, including whole night polygraphic recording. The tools for polysomnography have offered valuable experience in dealing with issues related to data from long term monitoring (8 hours). Beyond the known strong interdependencies between sleep and epilepsy [47], additional justification for studying normal sleep microstructure features has been given by recent findings linking epileptic ictogenesis to sleep and more specifically to sleep instability [48], sleep K-complexes and sleep spindles. The results of these offline data analyses provided new insights into different aspects of epilepsy and sleep, and were relied upon to offer recommendation of the polygraphic online monitoring of patients.

Every online recording performed with the ARMOR online platform system is uploaded to the Patient Health Record (PHR) database. From there it is transferred to the offline analysis database. In order for this service to be precise, there are several steps that should be followed. The first one is to check if there is a new recording in PHR. It should be noted that every recording is related to a specific patient, a specific device performing the recording and the data of the recording. The synchronization service checks in specified time intervals for a new recording in the PHR system. If a set of new recordings is detected, then these recordings are requested from the PHR database. The format of the data in each new recording is Unisens. Once the whole recording has been downloaded and checked for errors (e.g. download errors, missing files etc) the data are transformed in EDF format. Once this step is completed a subroutine will handle the EDF data to extract all the necessary info and store them in the offline analysis database. Then the newly uploaded data can be accessed through pre-specified queries.

In the following figure the structure of the main components of the synchronization of the two databases is presented.

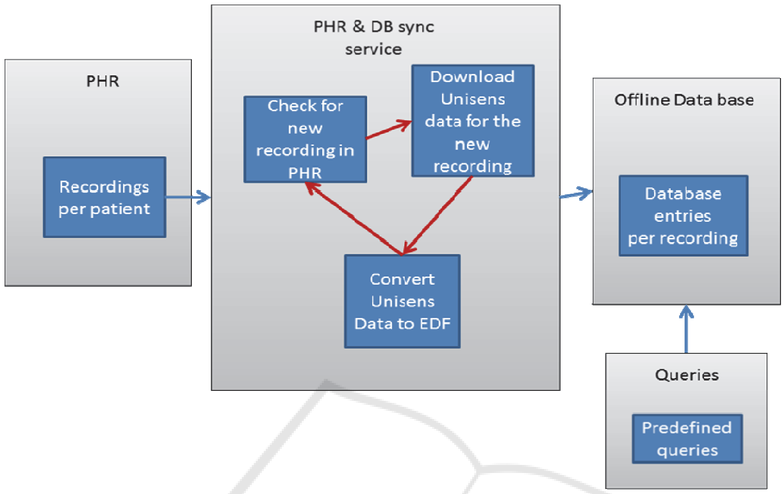

Fig. 5. Main components of the database synchronization.

3.3 Online Data Analysis Algorithms

One way of performing an online analysis of sensor data is a multi-layer Data Mining Model. These models are divided into four layers: *data collection*, *data management*, *event processing layer* and *data mining service layer*. The ARMOR Online platform is consisted of a similarly structured system. The data collection layer includes the sensors and uses the xAffect tool for streaming the sensors' data to a StreamInsight application. The streamed data are being processed with a previously specified and parameterised algorithm, before the detected events are extracted.

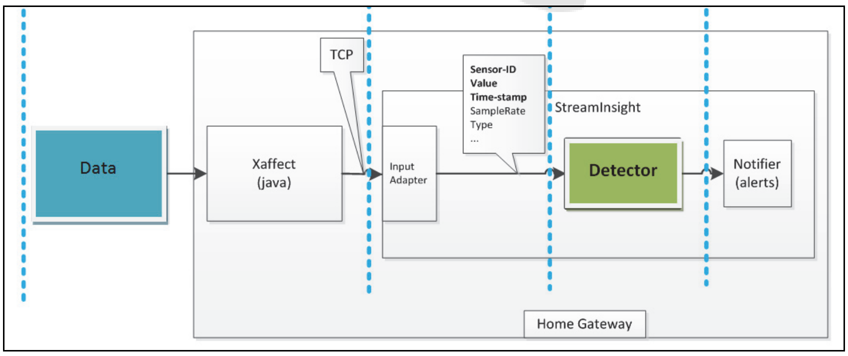

Fig. 6. Interface between different data management modules.

The core of each detection algorithm is implemented in Mathworks' Matlab environment. Matlab offers many features that make the design of an algorithm more efficient and effective as well as shortening the time needed for the development of the algorithm. An online application on the other hand requires a Data Stream Management System (DSMS), which offers the ability to process online data in a time and memory efficient way. The system used in our applications is StreamInsight from Microsoft. To introduce our algorithms to the Microsoft's StreamInsight environment, the .NET compiler and API of Mathworks have been used. In more detail, Mathworks provides a compiler for .NET packages. The result of this procedure is a set of libraries containing the algorithms and all the necessary components (functions, data such as training models, etc) necessary for each algorithm. The compiled libraries can be accessed by a StreamInsight application using the API that Mathworks provides. This API is the Matlab Compiler Runtime, which provides all the necessary components in order to use the algorithm in a stream application.

It should be noted that each algorithm has been designed to operate with segments of the data, as it is necessary in an online application. In order to pre-process, the streamed data, before having them processed from the detection algorithm, a set of StreamInsight tools were used. Depending on the procedure followed by the detection algorithm, the streamed data should be aggregated or transformed in matrices whose rows and columns correspond to channels and samples of each segment, respectively. The detection procedure is performed after this step. In the case of the seizure detector for each time window of the streamed data, a matrix should be formed. Each row of this matrix contains the data values for one channel during the specific time window, whereas the columns of this matrix contain the values for all channels for a specific time point. This transformation is possible due to StreamInsight's service of User Defined Operator.

4 Conclusions

As detailed in the previous sections, ARMOR project has addressed various critical, challenging and multifaceted objectives in order to effectively acquire, manage and analyze large number of signals related to epilepsy monitoring and decision-making. In order to offer such capabilities significant research, design and development efforts have been devoted to different and diverse areas ranging from pure medical research to engineering areas such as wireless sensor networking and data processing algorithms.

In that respect, this chapter attempted to highlight the main issues tackled and presented the main achievements as well as the design aspects of ARMOR project. Initially, the main architectural goals of ARMOR platform were presented, focusing on its main components. Then, the requirements and characteristics of the sensors used was also presented, as well as the overall communication infrastructure employed for robust, efficient and secure end-to-end transfer of user sensitive personal data. One of the cornerstone components of ARMOR architecture, ARMOR middleware, was also detailed. ARMOR middleware resides in the home gateway of ARMOR, plays multiple roles in the monitoring process and provides diverse functionalities both related to communication and data processing. The second part of the chapter focused on data analysis processes and algorithms designed and developed in the context of the project so as to gain significant insight to epilepsy monitoring and decision making.

Concluding, ARMOR project proposed a highly efficient system able to offer significant assistance and advancements on epilepsy monitoring and decision-making exploiting state-of-art technologies as well as extending them.

References

1. Christian M. Korff. Ingrid E. Scheffer, "Epilepsy classification: a cycle of evolution and revolution", Curr Opin Neurol. 2013 Apr;26(2):163-7. doi: 10.1097/ WCO.0b013e32835ee58e.
2. ANNE T. BERG, J. HELEN CROSS, "Classification of epilepsies and seizures: historical perspective and future directions", Handbook of Clinical Neurology, Vol. 107 (3rd series) Epilepsy, Part I H. Stefan and W.H. Theodore, Editors, 2012 Elsevier B.V
3. Newton CR, Garcia HH, "Epilepsy in poor regions of the world", Lancet. 2012 Sep 29;380(9848):1193-201. doi: 10.1016/S0140-6736(12)61381-6.
4. Badea A, Kostopoulos GK, Ioannides AA. Surface visualization of electromagnetic brain activity.J Neurosci Methods. 2003 Aug 15;127(2):137-47
5. Barnathan M, V. Megalooikonomou, C. Faloutsos, F. Mohamed, S. Faro, «High-order Concept Discovery in Functional Brain Images», 7th IEEE International Symposium on Biomedical Imaging: From Nano to Macro (ISBI), Rotterdam, The Netherlands, 2010, pp. 664-667.
6. Barnathan M, V. Megalooikonomou, C. Faloutsos, F.B. Mohamed, S. Faro, «TWave: High-Order Analysis of Spatiotemporal Data», In Proceedings of the 14th Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD), Hyderabad, India, June, 21-24, 2010, Advances in Knowledge Discovery and Data Mining, Lecture Notes in Computer Science, 2010, Volume 6118/2010, pp. 246-253.
7. Iasemidis LD, Shiau DS, Pardalos PM, Chaovalitwongse W, Narayanan K, Prasad A, Tsakalis K, Carney PR, and Sackellares JC. Long-Term prospective on-line real-time seizure prediction. Clinical Neurophysiology 2005; 116(3):532-44.
8. Ioannides AA, Corsi-Cabrera M, Fenwick P, del Rio Portilla Y, Laskaris N, Khurshudyan A, Theofilou D, Shibata T, Uchida S, Nakabayashi T and Kostopoulos GK.MEG tomography of human cortex and brainstem activity in waking and REM sleep saccades. Cerebral Cortex, 2004;14(1):56-72.
9. Velis D, Plouin P, Gotman J, da Silva FL; ILAE DMC Subcommittee on Neurophysiology. Recommendations regarding the requirements and applications for long-term recordings in epilepsy. Epilepsia 2007; 48(2), 379-84
10. Stefan H., Hopfengärtner R.: Epilepsy monitoring for therapy: Challenges and perspectives. Clinical Neurophysiology 2009; 120:653-58.
11. Jones V.M., et al.: Biosignal and context monitoring: distributed multimedia applications of body area networks in healthcare. 10th Workshop on Multimedia Signal Processing in Cairns, 2008.
12. Zijlmans M., Flanagan D., Gotman J.: Heart rate changes and ECG abnormalities during epileptic seizures: prevalence and definition of an objective clinical sign. Epilepsia 2002; 43: 847–54.
13. Massé F., Penders J., Serteyn A., Bussel M. van, Arends J.: Miniaturized Wireless ECG-Monitor for Real-Time Detection of Epileptic Seizures. In: Wireless Health'10, San Diego, USA (2010)

14. Nijsen, T. M., Arends, J. B., Griep, P. A., Cluitmans, P. J.: The potential value of three-dimensional accelerometry for detection of motor seizures in severe epilepsy. In: Epilepsy & Behavior 7, 1, 74–84 (2005)
15. Poh M.-Z., Loddenkemper T., Swenson N., Goyal S., Madsen J., Picard R.: Continuous Monitoring of Electrodermal Activity During Epileptic Seizures Using a Wearable Sensor. In: 32nd Annual International Conference of the IEEE EMBS Buenos Aires, Argentina (2010)
16. Texas Instruments MSP430 microcontroller crypto software features informations:http://jce.iaik.tugraz.at/sic/Products/Crypto_Software_for_Microcontrollers/Texas_Instruments_MSP430_Microcontrollers
17. Somnomedics: http://somnomedics.eu/home.html
18. Medset telesmart: http://www.medset.com/index.php?id=45
19. Shimmer platform http://www.shimmer-research.com/
20. EU Directive: Data Protection Directive (Directive 95/46/EC), Directive on Privacy and Electronic Communications (2002/58/EC), Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare
21. MoviSens: http://www.movisens.com/en
22. Revoing2011: Revoking Networks "Advanced User Manual" Version 4.77 2/3/2011
23. SANS Institute InfoSec Reading Room , "Brush up on Bluetooth", 08/21/2003
24. George Krikis, Christos P. Antonopoulos, Nikolaos S. Voros, "Design and Implementation of Efficient Reconfigurable Cipher Algorithms for Wireless Sensor Networks" 11th IEEE International Conference on Industrial Informatics, Bohum, Germany, 29-31, July, 2013
25. Eichelberg M, et al. (2005), "A survey and analysis of Electronic Healthcare Re-cord standards", ACM Computing Surveys. 37(4):277–315
26. CEN/TC251–ISO/TC215 (2010), I. E. Electronic Healthcare Record (EHR) Communication. Parts 1: Reference Model, Part 2: Archetype Model, Part 3: Reference Archetypes and Term lists, Part 4: Security and Part 5: Inter-face Specification. 2010
27. Rector, A. et al. (1993), A framework for modelling the electronic medical record. s.l. : Methods Information Medical, 32: 109-119
28. Beale, T. (2002), "Archetypes constraint-based domain models for future-proof information systems", OOPSLA-2002 Workshop on Behavioural Semantics
29. Microsoft HealthVault (http://www.healthvault.com)
30. World Medical Card (www.wmc-card.com)
31. INDIVO Health (indivohealth.org)
32. TOLVEN Patient/Clinician HR (www.tolven.org)
33. OpenMRS (http://www.open-emr.org)
34. Schaaff K., Mueller L., Kirst M., http://www.xaffect.org/
35. Kirst M., Ottenbacher J., www.unisens.org
36. A. Bideaux, P. Anastasopoulou, S. Hey, A. Cañadas, A. Fernandez: Mobile monitoring of epileptic patients using a reconfigurable cyberphysical system that handles multi-parametric data acquisition and analysis: MobiHealth 2014
37. Hauser WA, Hesdorffer DC. Epilepsy: frequency, causes and consequences. New York: Demos Publications, 1990.
38. Pearce JL,Mackintosh HT. Prospective study of convulsion in childhood. The New Zealand Medical Journal 1979;89:1–3.
39. Elwes RCD, Chesterman P, Reynolds EH. Prognosis after a first untreated tonic-clonic seizure. Lancet 1985;2:752–3.
40. Hauser WA, Rich SS, Annegers JF, et al. Seizure recurrence after a first unprovoked seizure: an extended follow-up. Neurology 1990; 40:1163–70.
41. Berg AT, Shinnar S. The risk of seizure recurrence following a first unprovoked seizure: a quantitative review. Neurology 1991;41:965–72.

42. Crompton DE, Berkovic SF. The borderland of epilepsy: clinical and molecular features of phenomena that mimic epileptic seizures. Lancet Neurol 2009; 8: 370-81.
43. Stephenson JBP. Fits and faints. London: MacKeith Press, 1990; Lempert T. Recognizing syncope: pitfalls and surprises. J R Soc Med 1996; 89: 372-5.)
44. Hammill SC. Value and limitations of non-invasive assessment of syncope Cardiol Clin 1997; 15: 195-218
45. Kapoor WN. Evaluation and outcome of patients with syncope Medicine 1990; 69: 160-75
46. Kapoor WN, Smith MA, Miller NL. Upright tilt testing in evaluating syncope: a comprehensive literature review. Am J Med 1994; 97: 78-88
47. Kokkinos V, Koupparis A, Stavrinou M and Kostopoulos GKThe hypnospectrogram: An EEG power spectrum based means to concurrently overview the macroscopic and microscopic architecture of human sleep. Journal of Neuroscience Methods 2009; 185(1):29-38.
48. Halasz P, Kelemen A. Relationship of phasic sleep phenomena, spike-wave discharges, and state-dependent responsiveness in sleep. Epilepsia. 2010 May;51(5):934-5.
49. Eric Conrad, "Advanced Encryption Standard", WhitePaper