Department of Economics Democritus

University of Thrace

Interreg
Greece-Bulgaria
eHealth Monitoring
European Regional Development Fund

EUROPEAN UNION

D4.3.2 APPLICATION/ SOFTWARE DEVELOPMENT

(Software Engineer -Developer)

«Healthcare Monitoring System Design»

Reporting period: 20/09/2018 - 30/08/2020

WP 4 Joint Monitoring System

project

IMPROVING HEALTHCARE ACCESS THROUGH A PERSONAL HEALTH MONITORING SYSTEM

George Pistikos

August 2020

The project is implemented in the framework of INTERREG V-A "Greece-Bulgaria 2014-2020" Cooperation Programme and is co-funded by the European Regional Development Fund (ERDF) and by national funds of the countries participating in the Programme

http://www.ehealthmonitoring.eu/

Summary

According to the contract (14/09/2018, Ref. No: 44956) for the project APPLICATION/ SOFTWARE DEVELOPMENT, the deliverable «Healthcare monitoring system design» that is being implemented within the frame of WP 4 Joint Monitoring System of the project IMPROVING HEALTHCARE ACCESS TROUGH A PERSONAL HEALTH MONITORING SYSTEM under the INTERREG V-A Greece – Boulgaria 2014-2020 Programme, describes the activities that have been carried out within the period 20/09/2018 - 30/08/2020.

The work of the period focused on the study of the security requirements of the system and on the formulation and implementation of an integrated Information Security Policy. Initially, the document presents the design of an integrated system for record and analysis of biosignals that facilitate effective patient monitoring at home. The main contributions of the system are the standardization of biosignals collection and the introduction of Cloud Computing concepts and tools for data managements and analysis utilizing point-of-care decisions. Part of the deliverable is the study that has been conducted for the development of an innovative and interactive integrated service of health monitoring.

Furthermore, it describes the final version of the system architecture. The main requirements for the security, confidentiality and integrity of the sensitive personal data kept, the certification of users, as well as the compliance with the national and Community legislation are presented. Then, the Information Security Policy and the technical and organizational characteristics of the Security System are presented.

Table of Contents

Table of Figures

1 Introduction

Direct provision of healthcare and follow-up services, or the so-called point-of-care service, is seen as a key issue for improving the quality of life, especially for older people. Mobile penetrating healthcare technologies can support a wide range of applications and services, including mobile telemedicine, independent living, site-based medical services, emergency response, personalized monitoring and access to healthcare information, providing significant benefits to both patients and medical staff. However, implementation of the management of health-related information via mobile and wireless devices involves several challenges, such as data acquisition, storage and management (e.g. different devices, different communication protocols, physical storage issues, availability and maintenance), interoperability and availability of heterogeneous resources, security and privacy protection (e.g. controlling license, data anonymity, etc.), unified and generalized.

The trend in modern personal monitoring systems is the use of Cloud Computing Template [2]. Cloud Computing provides access to shared resources and shared infrastructure in a generalized and diffused manner, offering on-demand services over the network to perform functions that respond to the changing needs of electronic healthcare applications. In this context, we have developed an integrated homeowner health monitoring system that uses the Cloud Computing infrastructure to manage and analyze data. The proposed solution focuses on the functionality of system decision support, which is implemented both in the smartphone application for temporary analysis and Cloud.

The rest of the document is structured as follows: Chapter 2 presents the relevant research and discusses basic information about Cloud Computing and the final version of the system architecture. Chapter 3 presents the approach adopted for biosignals life cycle and data modeling as well as the main APIs of the application stack. Chapter 4 presents the describe the system and technologies on which it is based and the requirements regarding data security and confidentiality, as well as the information system security study, which analyzes the characteristics of the security system. Chapter 4 also lists the proposed procedures for detecting and managing security incidents.

2 Related Research and Integrated Health Monitoring System

2.1 Related Research

Various health information systems have already been identified and established to monitor and assist chronic patients, the elderly and people with disabilities. The use of biosignals is considered necessary to understand the health status of a person in such systems. In this context, the credible acquisition, gathering, and safe transfer of biosignals data or any kind of medical data to remote computing infrastructures are the greatest challenges during the installation of a point-of-care system. The widespread use of mobile devices with significant online and computing capability has allowed them to be used as intermediate nodes or nodes - portals limiting the need to integrate sophisticated networking technologies into specialized medical devices. The three-tier model, consisting of i) biosignal sensors, ii) biosignal gates and circuits, and iii) the Cloud infrastructure allows efficient hardware utilization and low-cost communication.

Sensor device makers focus on acquiring effective biosignals while using standard wireless short-range technologies to transmit data. Biosignal portals and circuits can be implemented using mobile or embedded platforms with off-the-shelf operating systems based on sophisticated technologies such as REST services and TLS security for reliable and secure transmission to the cloud infrastructure. An important issue is the compatibility between health devices and gateway nodes, which introduces complexity especially in the design of the gateway node.

Extensive biosignal analysis goes beyond the scope of this document, but we are addressing some key issues to highlight the diversity of communication methods, including media and protocol specifications, data exchange styles and available APIs for managing sensors.

Biosignal sensors mostly transmit their data via Bluetooth and USB, and the use of the mini-jack is also seen for some types of sensors, such as glycosylates. However, even in the case of using Bluetooth, different Bluetooth protocol specifications are available and only a subset of them is applied by sensors and computer and receiver devices. The two main versions of Bluetooth communication can be described as (a) the classic Bluetooth standardized by IEEE 802.15.1 as well as b) Bluetooth Low Energy - BLE (or Bluetooth Smart). The BLE, derived from the Bluetooth 4.0 version, is considered to be a major breakthrough that allows for more efficient data transmission, lower power consumption and simplest communication processes compared to classic Bluetooth that needed to match finds and prepare before biosignal data exchange. The BLE software model introduces the concept of Generic Attribute Profile (GATT), which is a general API for communication with any BLE device. The model also offers a number of special profiles for certain types of devices and communication purposes such as placement, healthcare, headset communication, etc.

The ISO / 11073 IEEE [3] standard provides a framework for the connectivity of health devices to the use of wired (USB) or wireless short-range communication technologies (Wi-Fi, Bluetooth, Zigbee) on gate devices. Nonetheless, healthcare device makers have built up short-range wireless connectivity relatively recently and practically, many still use proprietary protocols to transmit cloud data through apps that run on Android or iOS platforms via cable (USB) or wireless (Bluetooth) physical layers.

Continua Health Alliance [http://www.continuaalliance.org] has proposed a framework to promote interoperability between ISO / IEEE 11073 and BLE devices. However, the use of specific communication profiles and healthcare standards for the time being is limited.

Instead, manufacturers often use proprietary GATT protocols to communicate with BLE sensors, or low-level messages to communicate with classic Bluetooth sensors.

The abundance of available devices, where each manufacturer follows different communication standards and implements non-standard data formats, gives tremendous complexity to third-party tools and applications for the communication and use of such sensors. In addition, different types of biosignals and different measurement techniques raise additional challenges for communicating with sensors and acquiring and managing biosignals data. For example, pulse oximeters provide streaming data, while blood pressure monitors provide uniform results of measurements, and in this sense, the devices connected to them should provide different detectors for acquiring and managing data.

It is well known that sensor manufacturers provide specific APIs to communicate with their products by breaking access to Bluetooth components to provide better control and communication performance to them. However, incorporating multiple protocols and APIs from manufacturers into the same software as a smartphone app is not always easy due to compatibility and aggressive use of resources and services from each API library.

A variety of architectural systems have been presented in the literature and different aspects of these systems have been evaluated. More specifically, the research of wireless interconnection protocols is presented in, and can be used for common health devices such as blood pressure monitors and pulse oximeters and various machine-to-machine (M2M) architectures and collection health data.

Researchers also propose an IEEE 11073-based architecture that uses "Personal Health Managers-PHI" and works close to the user and also suggests "Internet Health Managers" based on cloud infrastructures and communicates with PHIs by evaluating the use of CoAP for transactions. Bluetooth health sensors (pulse, oximeter, and ECG) are also used to communicate data with an Android device, which then transfers to the server with the MQTT connection protocol. The ability of Android mobile devices, such as resource gates and battery life effects, is estimated at.

The findings highlight that mobile devices can play this role, however battery life can be greatly affected. Finally, the present deliverable evaluate home screening technologies with clinical trials and identify key performance characteristics and regulatory requirements in a home-based telemonitoring platform. The bibliography highlights the need for greater accuracy of health devices and suggests online support by trained specialists for filtering and interpreting data collected.

As far as decision support is concerned, there are several techniques for identifying patterns and sorting data for biosignal analysis. More specifically, there is a variety of classification methodologies ranging from classic statistical methods, such as linear and accounting regression or Bezijski networks, to more sophisticated artificial intelligence techniques, such as neural networks and genetic algorithms, or the latest support vector machines. Other types of hybrid intelligent systems are neuro-fuzzy adaptive systems, which may consist of an adaptive fuzzy controller and an internet-based predictive marker. The challenge for such smart systems lies in the complexity of capturing, representing and processing biosignals data to produce knowledge.

In addition to presenting the information, we want the orders to be executed automatically as well as to reform the system on behalf of the user, depending on the changes in the decisions.

For example, in the event of a user's health deterioration, the intelligent system needs to be able to respond by activating an appropriate alarm and providing corresponding indications that explain why the corresponding alarm is triggered. Appropriate training and calibration of artificial intelligence modules is required in advance.

2.2 Integrated health Monitoring System

The project platform provides high quality medical monitoring and communication services through immediate response and accurate recording of biomarkers and other critical information, serving the ever-changing needs of the elderly and chronically ill in the field of so-called mhealth services. Through the supported services, the end-users' compliance with the care obligations is enhanced and an increased sense of security for the patient himself, but also for his relatives. In addition, the system is minimally invasive, offering a unique user experience.

In addition, the platform facilitates the creation of a human-centered support network of health professionals, relatives and friends of patients and also provides the framework and services needed to effectively communicate and manage a wide range of wearable devices and sensors, enabling the seamless monitoring of biomarkers and user activities.

The end user can use biomarker recorders and / or wearables, depending on their needs, while the mobile application requires a tablet. The treating physician can connect to the system from his computer and assess the patient's state of health and evaluate the Electronic Medical History (demographics, medical history, laboratory test results, drugs, allergies, etc.).), using the analysis and

imaging tools of the platform, and consequently can determine the monitoring features and treatment regimen that fits the patient profile. The system allows the creation of a special personalized schedule of measurements which should be taken and entered into the system on a daily basis, either manually by the patient or automatically from the sensor network, the respective permissible limits of each biomarker for the detection of an emergency or a abnormality, as well as the prescription drug and the medication schedule. Compliance with the treatment regimen and personalized monitoring program is implemented through reminders on the tablet.

The system processes the data related to the schedule in the Cloud and whenever a measurement exceeds the limit set by the treating physician, the physician is informed through a default communication channel (push notification, e-mail, etc.) and can if he wants to communicate directly with the patient. This is achieved by utilizing the function of video conferencing that offers the possibility of social networking with the "care cycle" of the user either in the form of communication with friends and relatives or with medical staff in normal cases and emergencies.

The basis for the proposed decision-making approach is illustrated in Figure 1. The proposed platform allows the creation of a patient-centered health care support network and also provides the framework and required services for the effective communication and management of a wide range of device and sensor wearers that allow for the continuous monitoring of patient's activities.

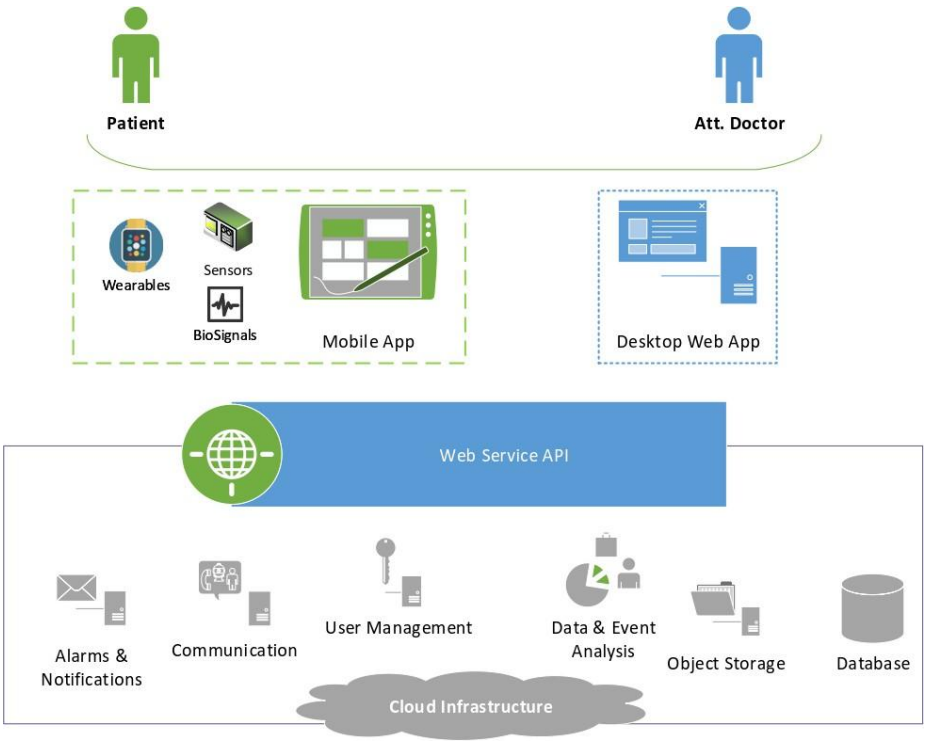

Figure1 Integrated Health Monitoring Platform

2.3 System Architecture

The service information system consists of a set of servers. The servers, paired to achieve high availability, perform the following functions:

- High Availability Proxy: Ubuntu Linux 18.04 LTS (http://www.ubuntu.com/) will be installed on two servers on which hapapxy (http://haproxy.1wt.eu/) will be installed as well as its pacemaker Linux High-Availability project (http://www.linux-ha.org). The two servers act as an active-passive cluster and the failover from one to the other is taken care of by the pacemaker, so that the operation of the information system continues smoothly even in case of complete software or hardware failure of one of the two servers.
- Web Servers: Two servers with Ubuntu Linux 18.04 LTS installed work as web servers using an architecture with a NGINX Web Server in front (Proxy) of a NodeJS Web Server. Haproxy determines who will be the active NGINX and who will be the backup inactive. NGINX is equipped with various modules and works
    - as a Loadbalancer that shares the load on NodeJS servers,
    - as a Web Application Firewall, filtering the communication and making quality controls on the incoming packages, shielding the system from a variety of attacks (mod-security, mod-evasive)
    - as an SSL-Offloader, decrypting SSL communication before forwarding data to NodeJS servers, thus improving their performance.
- Database Servers: Two servers with Ubuntu Linux 18.04 LTS installed have MySQL Database Server installed. To ensure high data availability, both databases are replicated in Master / Slave wiring. Haproxy acts as a loadbalancer and directs read / write processes on the master database server and read processes on the replicated slave database server, improving database response times.

Availability of services is ensured by the infrastructure and the management services of these infrastructures offered by the cloud service provider.

- Firewall: The firewall of the cloud service provider prohibits any connection to the servers. Only authorized users have access to the system via SSH. Only a minimum number of ports are allowed to be connected, which must be open, e.g. ports 80 and 443 on Web Servers are accessible to everyone.
- Network Storage: Storage of data accessible from the virtual machines that implement the service, using the object storage service, which offers 99.99% availability, 99.999999999% durability and great ease of system expansion. In addition, there is a system for identifying and managing user access to object storage data.

3 Life Cycle and Data Modeling

In order to design and implement a framework for the measurement, management, storage and analysis of biosignals, it was necessary to first study the lifetime of a biosignal once it is taken for permanent storage in a repository of a base data. This life cycle extends to various frame components, both in the patient environment and cloud computing.

The various functions on the patient's side are performed in an application that is responsible for:

1. the capture of biosignals by the various sensors using specific movements applied to each sensor,
2. aggregating the metrics and converting them into a common model and common format,
3. performing a temporary analysis to evaluate the quality of each measurement and
4. periodic synchronization of measurement data with the cloud platform.

In the suggested framework, we have chosen to use only sensors with a Bluetooth network interface. The thought behind this option is as follows::

- ✓ Bluetooth is available on all modern computing devices, smartphones and tablets,
- ✓ is easy to use,
- ✓ does not require additional wires or equipment, greatly improving the user experience and
- ✓ provides the required performance and capacity to manage biosignal data.

From the cloud computing side, platform components perform heavy computational operations for all patients, focusing on:

1. the acquisition of biosignals for applications,
2. their storage,
3. analysis that consolidates multiple parameters, models and real-time bio-data or historical data, and finally,
4. the reporting of the results of analyzing and supporting decision-making in emergencies and communication with appropriate services and staff.

4 Technology and Security Design

The Integrated Health Monitoring System consists of four main sub-systems that realize the required functionalities, as well as a cloud back-end platform, which supports all other subsystems. These subsystems have been designed and developed utilizing a rich set of state-of-the-art technologies and tools, in order to secure optimal levels of robustness, security and extendibility and the finest user-experience.

The system follows a service-oriented architectural design, exploiting the advancements and flexibility of cloud offerings, and implements modern UIs for all types of users. Cloud Computing allows for ubiquitous access to shared resources and common infrastructure, offering services on-demand, serving the constantly changing needs of the health-centric digital services. To that end, is being developed an integrated system for patient monitoring at home, utilizing Cloud Computing concepts and tools for data managements and analysis. The proposed solution focuses on the system decision support functionality, which is utilized within the smartphone app for initial assessment, as well as in the Cloud.

A combination of Java and JavaScript technologies and frameworks are used for implementation and communication of the various application components and services. A cross-layer technology that has a key role on the realization of the communication and videoconferencing functionality is WebRTC, which is used both for the desktop and mobile applications. The applications used are:

- Android App
- Web App
- Cloud Platform

4.1 Requirements

In the case of a digital or information system, such as the design of a Health Monitoring System, data security and access to data may be related to:

- Technical (for example, user authentication, access control or data encryption)
- Physical level (where the data is stored and who has access to the specific space)
- Organizational (control and certification of those who have access to the system or data, obligation to comply with security procedures, data recovery plan) and
- Legal (arising from the obligation to comply with relevant laws and regulations, such as the GDPR)

The goals of the security system are summarized in the acronym CIA: Confidentiality, Integrity and Availability. Confidentiality refers to preventing data leakage without certification. This practically means that only the certified recipients of a message or the operators of an action should have access

to or the ability to complete the action. In the case of integrity, the systems should prevent the alteration or destruction of the information without the relevant certification, while the users should have the relevant sense of confidence that they will retrieve the information in the same way and with the same content with which they introduced it. Therefore, any change or destruction of information should only be done by users who are certified to do so and in accordance with the procedures set out in the security policy. Finally, availability refers to the need for the data to be available and usable by certified users in a timely manner and in a way that does not interfere with the smooth operation of the system and the day-to-day operations of the organization. This means that, in addition to the technical response of the system, some process of preventing data from being hidden from users who are certified to retrieve it is necessary (for example, due to a long delay in a data report).

With regard to authorized access to information, in most cases such systems rely on the OAuth 2.0 protocol, which implements the above requirements, especially in conjunction with an existing directory infrastructure (LDAP). Through software running on the server (server-side) such as KeyCloak, we have the ability to define user groups with specific data access and processing capabilities, while through the OAuth 2.0 authentication protocol, access to the system information of unauthorized users is prevented, at the web page level.

Regarding GDPR, which expands on the previous legislation in force (Law 2472/97), the system should support the following functions:

- Systematic and clear information of all system users on the data held and obtaining consent
- Detailed description of the data kept, especially if it is data related to the patient's physical or mental health, and the level of health services offered to the patient
- Data leak detection procedures and timely and clear information of users who may be involved (in less than 72 hours)
- The ability of users to request the deletion or anonymization of their data in the system. In the latter case, the data can be retained, but without an identifier (eg name or password) that can help locate the user.

4.2 Roles and Responsibilities

The Security Administration is created and the role of the Security Officer for the central management and coordination of the security issues of the system. The responsibilities of the Security Officer more specifically are the following:

- Carrying out checks that confirm the existence of the desired levels of security in the different technologies that make up the application such as:
    - Servers
    - Databases

- Web Application

- Evaluate and comply with the results of external security audits by third parties regarding the application.
- Periodically check logs for possible attacks or illegal access.
- Design a secure backup process.
- Ensuring the integrity of backups and logs.
- Conduct periodic audits to ensure the implementation of safe practices at all levels of use and application management by the security team.

4.3 Security Policy

4.3.1 Security Principles

The service provider is obliged to:

1. Have and maintain access policy for systems that refer to external connections, data communications, telecommunications devices and software programs.
2. To take all necessary and appropriate measures for the protection of its facilities, for the control of access, so that it is allowed only to authorized persons.
3. To inform users about the protection measures they can take to ensure the confidentiality of their communications and data, e.g. the use of specific software or encryption technologies.
4. To inform users about communication data that may be stored in backups but also to notify them of the maximum period for which the data will be stored.
5. To take into account and apply in its policy section the provisions of the legislation for the processing of communication data.
6. To use systems to strengthen the protection of the network, 24 hours a day. Interruption of these systems is allowed only in cases of maintenance or failure.
7. Develop and maintain a system contingency plan after malicious attacks including backing up, providing emergency resuscitation procedures, and recovering from an attack. In addition, deliver the latest Backup Policy each time a major change is made to it.
8. To have a clear Security Incident Handling Procedure (IFRS) for incidents which threaten the security of the communication infrastructure but also to ensure the confidentiality of the communications carried out through the provider. In addition, it must renew it and check at regular intervals the readiness of activation of all mechanisms and persons of the IFRS as well as hand it over to the competent authorities in each audit.
9. To have a network security control team and during the controls, to allow access to the network as the level deemed necessary for their execution as well as an Virus response team that will be able to refer a user who needs help, to the competent company when requested.

4.3.2 Health Information Security Policy

Users of the system have rights to the protection of their personal data and the confidentiality of data transfer related to the management of their care. Any remote provision of care to users of the system must be made in an appropriate environment that guarantees the absence of unrelated persons. System users should be aware of the presence of others on the other end of the video conferencing system, even if they are not visible to the camera.

Users of the service, or members of their families, should also be informed of any electronic or magnetic storage of the teleconferences and approve it orally or preferably in writing.

Greek legislation, following Directive 95/46 / EC, through the provisions of Law 2472/97 and its amendments, describes the general legal framework governing the use of sensitive personal data. Within the framework of the service, special care has been taken for the faithful observance of this legal framework, recognizing that, especially the medical data, they are extremely sensitive.

The following rules are followed especially for medical data:

a) The patient has expressly given his consent, or
b) Treatment is necessary to safeguard the patient's vital interest while he or she is physically or legally unable to give his or her consent, or
c) The treatment is necessary for medical prevention or diagnosis, the provision of medical treatment or the management of medical services, and the treatment is performed by a health care professional who is bound by medical confidentiality or by another person who is subject to such obligation.
d) The controller must inform the patient of the purpose of the treatment, the data necessary for that purpose and the recipients of the treatment, whether the treatment is compulsory, and of the existence of a right of access to his data.
e) The patient has the right at any time to request to be informed what personal data and for what purpose have been processed.
f) The patient has the right to correct and delete the data if it is not accurate or the processing is not legal.

4.3.3 Information Security

With regard to the design of the Integrated Health Monitoring System, the selection of appropriate Information and Communication Technologies (ICT) ensures:

- Certification: verifying the authenticity of the identity of the parts of a data exchange.
- Authorization: user access must be authorized.

- Confidentiality: maintaining the confidentiality of data.
- Integrity: the data must remain intact, ie not distorted.
- Non-refusal to participate: the user should not be able to refuse to participate in the data exchange.
- Controllability: any modification or processing of data must be controllable, ie by whom and when.
- Responsibility: it must be clear who is responsible for entering, accessing or modifying any data.
- Transparency: the processing procedures must be documented so that they can be checked.
- Availability: data should be available when needed.

4.4 Information Security System Specification

The platform that hosts the application of the Service consists of individual parts of software and hardware and for this reason the features of the security system are divided into the following parts: Server Software Protection, Network Protection, Database Protection, Backup Process, Secure Communication of the service with the User. It should be noted that the application is web-based and for this reason mechanisms are implemented for secure communication on the Internet.

4.4.1 Server Security

The first security feature refers to the protection of web application server software. This protection is achieved in the following ways.

- Installation and use of advanced operating systems: Ubuntu Server 20.04, one of the most common, stable and secure operating systems for servers, is installed on the servers.
- Controlled user access and periodic change of administrator password: Software servers can only be accessed by specific IPs and specific users, whose passwords change every 2 weeks.
- Recording of user actions: Users' actions are recorded in order to control and correct faults but also to provide security through the detection of malicious actions. Specifically, the log is made in special files (log files), which contain in an appropriate format information about when and by which user a specific action was performed. Logs are divided into operating system, web server, and application levels, ensuring that the actions of all users who come into contact with the system in any way are recorded.

4.4.2 Software Updates

The schedule for installing the updates is as follows:

- Critical or important updates, which are directly related to the subsystems used by the application and therefore it is immediately possible to exploit the vulnerabilities to be fixed by malware or users, are installed immediately.
- Security updates, which concern operating system fixes to subsystems that are not used directly or indirectly by the application and are not exposed through the network to third party users are installed 3 days after their publication, to allow a short test time by the general public and to avoid any malfunctions.
- Functionality updates are installed at the discretion of the administrator and at a time specified by him after it is confirmed that they do not disrupt the existing functionality of the application.

Updates are installed on servers starting with the least critical of each pair of servers. The above procedure ensures the overall functionality of the application. Even if a server has a problem due to the installation of an update, the other server in the pair will continue to run until the cause of the problem is found and corrected.

The security and functionality updates of the Operating System as well as the software installed on the servers (Web server, Database server) are made with the same philosophy, i.e. according to their criticality and always gradually in pairs. The apt tool is used for Linux server subsystems.

4.4.3 Firewall

To protect the network, prevent attacks and regulate data traffic, the platform is protected by a strong firewall provided by the cloud service provider. Each server of the platform is protected by a different firewall. Firewalls are configured to reject all connections except those allowed by the network administrator (default deny). The following have been taken into account during the installation, configuration and management of firewalls:

- Firewalls are configured to protect the network from malware. They only accept the required protocols and IP addresses.
- The firewall is managed only by authorized persons through a special management page with a powerful access control protection system. In addition to the administrator password, a special device is required which generates temporary passwords and is synchronized with the servers of the cloud service provider.
- All attempted network breaches are recorded and monitored.
- Successful and failed firewall access attempts are logged and controlled by the cloud service provider.

- Passwords change monthly.
- Firewalls are controlled by a special part of the cloud service provider which controls their operation and installs all the necessary security updates.

All connections and firewall checks are regularly reviewed and reviewed for security issues.

Firewalls that protect servers from external access also control access from the internal network. As with the external network, they allow access to specific ports to be restricted, maximizing security and tolerance for various cyber attacks.

To protect the system from Denial of Service or Distributed Denial of Service attacks, the necessary settings have been made in Apache Server and special Modules such as (Mod_Security, Mod_Evasive, etc.) have been installed.

4.4.4 Database Security

Controlled access to the local Database (DB) is achieved by creating user accounts and restricting authorization, on the one hand, and blocking access to the local DB remotely, so that access is only possible from specific IP addresses of management subsystems.

4.4.5 Change Management Process

All changes made at the platform and application level are recorded in an SVN system. This way we have the following possibilities:

- Easy installation of new changes
    - Import, upgrade, delete files in a transaction.
    - Ability to upgrade files to groups to make them easier to sort and manage
- Complete history of files and all changes made to them
- No file lock
    - File locking has proven to be inefficient, which is why SVN provides conflicting file-finding capabilities and merging tools to cover the most demanding cases
- Ability to retrieve older versions in real time during the commit process
- Possibilities of branching and tagging as well as merging with each other
- Maintaining log files for any changes that are made and easy access and management

4.4.6 Backup Procedure

The backup process ensures maximum recovery of application and user data in case of data loss. Data loss status may occur:

- From error state on server storage media (Hard Drives)
- From deleting files incorrectly

- From a power outage that may be accompanied by a fault in the storage media
- From natural destruction of the hosting space of the hardware (H/W) of the application (servers, databases, etc.)

Backups are treated as of equal importance to active data. Therefore, the same security policies are applied in all storage areas that protect the database data. The backup process is done automatically and at regular intervals to minimize data loss in the event of errors and natural disasters.

The data that is considered necessary for backing up is that contained in the Database. Specifically, a full backup copy of the database is received daily, as well as a copy of its logs every two days. More specifically, full backups are received every night and incremental backups every 4 hours.

Shortly after each full backup (every night), a compression and encryption process is performed (7zip application with AES256 encryption) of all day backups.

4.4.7 Secure Communication with the User

Medical confidentiality is enshrined in article 371 of the Penal Code, the Regulation of Medical Ethics (B.D. of 25/5/1955), as well as in article 47 (6) of N. 2071/92 where the secrecy of the medical file is enshrined. Secure communication between the application service and the user includes the encryption of user data and parameters as well as user authentication. Authentication and encryption are done through Secure Sockets Layer (SSL) and Digital Certificates.

The communication between the cloud server and the server where the data of the medical records are available is done through web services that run on secure SSL connections. Also, it is possible to retrieve medical history only from the specific IP where the application server is installed.

The biosignals are sent from the devices to an Android application which through web services forwards them to the cloud application server. Data is sent via SSL. The data is encrypted on the mobile device and decrypted on the server.

4.4.8 Communication via SSL

Communication via SSL is done on the user's side through the browser, while on the web server there is a digital certificate installed with a key length of 2048 bits and all the appropriate settings have been made.

The SSL protocol is designed to provide confidential communication between two systems, one of which acts as a client and the other as a server. Confidentiality is ensured by encrypting all messages at the SSL Record Protocol level. It also provides mandatory certification of server identity and optionally client identity, through valid certificates from trusted Certificates Authorities. It supports a variety of encryption mechanisms and digital signatures to address all different needs. Finally, it ensures the integrity of the data, applying the technique of Message Authentication Codes (MACs), so

that no one can alter the information without being perceived. All the above are done in a transparent and simple way.

4.4.9 Password Management

Passwords are an important aspect of computer security. It's the first line of defense for user accounts. An unlucky code can result in exposure of the entire organization's network.

Regarding the security and correct use of the codes, the following applies:

- Users who must have their own personal passwords must first obtain a temporary secure password which they are required to change immediately afterwards. In case a user forgets their password and needs to be given such a temporary password, this should be done after verifying the user's identity.
- Temporary passwords are given to users securely.
- Passwords are not stored on computer systems in unprotected form.
- All user-level and system-level passwords comply with the general instructions for creating strong passwords.
- Users must follow good security practices when choosing and using passwords. All users are advised to:
    - keep passwords confidential
    - Avoid writing down codes on paper, unless this can be safely stored.
    - change password whenever there is any indication of possible system or password exposure
    - select quality codes with a minimum length of eight characters which are:
        - easy to memorize
        - they are not based on something that someone else can easily guess or retrieve using user-related information, e.g. names, telephone numbers, dates of birth, etc.
        - Do not have consecutive identical characters or groups of only numeric or only alphabetic characters
    - avoid entering codes in automated login procedures, e.g. stored in macros or shortcut keys
    - do not share codes used, including assistants or secretaries
    - no password is revealed from the phone to ANYONE
    - The code is not referenced in front of others
    - the form of the code is not indicated (eg "my last name")
    - No code is revealed in questionnaires or security forms
    - does not share a password with family members.

- No password is revealed to partners during holidays

4.5 Security Incident Identification, Reporting and Management Procedure

Indicative security incidents include network attacks, intrusions, denial of service, problems caused by viruses (Viruses, Trojans), software vulnerabilities (software vulnerabilities), abuse of resources (etc.). λ.π.

The key roles for managing system security incidents are analyzed below:

- Security Officer
  - Develop responsible and effective procedures for dealing with security incidents.
  - Communication with the Management for Security Incidents issues.
  - Continuous training of the teams involved in the development and support of the application, the system administrators and the support staff (Security Team).
- Support Staff
  - Receiving and recording incidents, monitoring incident history and informing technical managers, producing and publishing reports and statistics.
  - Communicate with users who obviously have different levels of technology experience.
  - Availability on a 24-hour basis

The management of security incidents starts from their recording. These can be recorded either by the security team that checks the system for any incidents, or by the team of HelpDesk agents who record incidents that have been reported to them by system users. In the latter case, the agents are obliged to forward the incidents to the security team which is responsible for:

- their registration (creation of tickets)
- their solution
- informing the HelpDesk agents team about the proposed assistance to the user.
- Updating the ticketing database

5 Conclusions

In this deliverable, the final version of the architecture of the Integrated Health Monitoring System was presented in detail. The main APIs of the application stack, through which the various functions of the system are supported, were mentioned. In addition, the system requirements for the security of sensitive personal data were analyzed and a proposed security policy and incident management methodology were recorded.

6 References

[1] World Health Organization mHealth: New Horizons for Health through Mobile Technologies: Based on the Findings of the Second Global Survey on eHealth. Available online at: http://www.who.int/goe/publications/goe_mhealth_web.pdf

[2] Doukas, C., Pliakas, T., & Maglogiannis, I., Mobile healthcare information management utilizing Cloud Computing and Android OS. In Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE (pp. 1037-1040). IEEE.