CogWatch – Cognitive Rehabilitation of Apraxia and Action Disorganisation Syndrome

D2.3.2 Report on networks II

Deliverable No.		D2.3.2	
Workpackage No.	**WP2**	Workpackage Title	**System Device and Networks**
Task No.	**T2.3**	Activity Title	**Networks**
Authors (per company, if more than one company provide it together)		**Matteo Pastorino, Alessio Fioravanti and Maria Teresa Arredondo (UPM-LST), José M. Cogollor, Javier Rojo, Manuel Ferre, Rafael Aracil and José María Sebastián (UPM-ROMIN), Chris Baber, Martin Russell, Manish Parek and Emilie Jean-Baptiste (UOB-EECE), Ricardo Ruiz (RGB).**	
Status (F: final; D: draft; RD: revised draft):		**F**	
File Name:		**Cogwatch_D2.3.2_Networks_II**	
Project start date and duration		**01 November 2011, 40 Months**	

EXECUTIVE SUMMARY

This deliverable updates the definition of the CogWatch general architecture for the second prototype, starting from the software development described in *"D2.3.1 Report on networks I"*. Moreover, in this deliverable, a detailed definition of the communication and security protocols is presented. The improvement of the algorithms and protocols are defined based on the deliverable *"D2.1 Report on system specification"* whose objectives were the analysis of system specifications and the definition of the architecture, and the conclusions obtained from the evaluation of the first Cogwatch prototype reported in *"D4.1.1 Report on technical evaluation I"* and *"D4.2.1 Report on Healthcare Evaluation I"*.

The purpose of the report also provides a technical overview of the algorithms and protocols of the Second Prototype of the CogWatch System; which are classified depending on the function they provide. Thus, the CogWatch system is composed of three main subsystems, the *Client Subsystem*, corresponding to the patient side used to perform rehabilitation sessions, the *CogWatch Professional Interface*, used by the professionals involved in the rehabilitation process to monitor in real time the rehabilitation session remotely; and the *Server Subsystem*, in charge of supervising patient performance and progress in rehabilitation. The overall CogWatch architecture is defined, including a general schema and a particular description of the defined sub-systems through block diagrams, and a description of every implemented function.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

REVISION HISTORY

Revision no.	Date of Issue	Author(s)	Brief Description of Change
v0	10/06/2014	UPM	Table of Content
v1	24/06/2014	UPM	ToC modified, Executive summary, Introduction and first version of section 5
v2	15/07/2014	UPM	Internal contribution integrated.
v3	21/07/2014	UPM	Section 6 integrated
v4	22/07/2014	UPM, RGB	Update sections 3.1.1, 3.1.5 and 3.3.3
V5	30/07/2014	UPM	Update sections 3, 4 and 7
V6	15/09/2014	UPB,UOB	Update Sections 3, UOB contribution. Deliverable ready for the peer review.
FINAL	14/10/2014	UPM	Final version ready for submission

LIST OF ABBREVIATIONS AND DEFINITIONS

Abbreviation	Abbreviation
AADS	Apraxia and Action Disorganisation Syndrome
ACL	Asynchronous Connection-Less
AES	Advanced Encryption Standard
AM	Account Manager
API	Application Programming Interface
AR, AAR	Action recognition, Automatic action recognition
BAN	Body Area Network
CCS	CogWatch Client sub-system
CHS	CogWatch HealthCare sub-system
CM	Cue Manager
COM	Communication port
CPI	CogWatch Professional Interface
CSS	CogWatch Server sub-system
CWS	CogWatch WebPortal sub-system
DDoS	Distributed Denial of Service
DoS	Denial of Service
DSL	Digital Subscriber Line
FM	Fusion Module
HIH	HEALTHCARE Information Handler
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

ID	Identifier
IETF	Internet Engineering Task Force
IH	Information handler (within VTE)
IIS	Internet Information Services
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	IP version 4
IPv6	IP version 6
ISO	International Organization for Standardization
LAN	Local Area Network
LED	Light emitting diode
LMP	Link Management Protocol
MITM	Man in the middle
NIBP	Non Invasive Blood Pressure
OSI	Open Systems Interconnection
P1	CogWatch First Prototype
P1.1	CogWatch Prototype 1.1
P2	CogWatch Second Prototype
PAN	Personal Area Network
PNI	Pulse oximetry
SDK	Software development kit
TLS	Transport Layer Security
TM	Task model
TMI	Task model interface

USB	Universal Serial Bus
VPN	Virtual private network
VTE	Virtual Task Execution
WCM	Web Portal Communicator Module
WIH	Web Portal Information Handler
WLAN	Wireless Local Area Network
WPA	Web Portal Algorithm
WSDL	Web Services Description Language
XML	eXtensible Markup Language

1. INTRODUCTION

This deliverable is focused on the description of the developing software modules in the CogWatch system, together with the description of the communication, security and network specification. This deliverable is focused on the improvements of the P1.1 of CogWatch system including the specifications for the P2.

Considering that the structure and the main core of the system will be the same as in P1.1, many modules didn't suffer consistent modifications so, a specific reference to the previous deliverable (*D2.3.1 Report on networks I*) will be provided.

This deliverable aims at provide a technical overview of the architecture, the algorithms and protocols of the Second Prototype of the CogWatch System; which are classified depending on the function they provide.

CogWatch requires the development of ad hoc algorithms, able to identify and predict the errors made during the task execution. For this reason, dedicated modules have been implemented in order to analyse the data coming through different devices, described in the deliverable *"D2.2.1 Report on devices I"* and *"D2.2.2 Report on devices II"*.

This report is divided in six main sections, which describes the overall algorithms and protocols developed for the second prototype of the CogWatch system or the adapted version of the algorithms developed for the first prototype and adapted in the new one.

Section 2, describes the general architecture of CogWatch system, including an overall description of each sub-system and highlighting the differences with the defined architecture for the first prototype.

Section 3 describes the *CogWatch Client sub-system (CCS)* defined for the P2 with particular attention to the modules and algorithms developed for the first prototype. In the CCS, data are collected using the devices described in the *"D2.2.1 Report on devices I"* and *"D2.2.1 Report on devices II"*. Three main blocks are described in this section the *CogWatch VTE Interface*, the *VTE Local Repository* and the *CogWatch Configuration module*.

The *CogWatch Professional Interface (CPI)* is described in section 4.The CPI tool has been defined and developed to allow the clinical professionals to follow in real time the rehabilitation sessions remotely.

In section 5 a general overview of the *CogWatch Server sub-system (CSS)* is provided. Considering that no particular changes have been defined in the CSS, only the updated modules are described, while the unchanged modules presented in *"D2.3.1 Report on networks I"* are identified.

The communication and security protocols used to assure the personal data and the secure transfer of information between the different sub-systems of the CogWatch system are described in section 6.

Finally, section 7 presents the conclusion of the deliverable.

2. GENERAL ARCHITECTURE

The overall architecture of the CW system has been modified with respect to the architecture described in *"D2.2.1 Report on devices I"* and *"D2.2.2 Report on devices II".* The new architecture has been designed according to the technical improvements developed before the first technical validation of P1 and described in *"D4.1.1 Report on technical evaluation I"*.

The first version of the CW was composed of two different subsystems, the *CogWatch Client sub-system (CCS)* and the *CogWatch Server sub-system (CSS);* while the *CogWatch Professional Interface (CPI)* has been added in the second version (v1.2) of the prototype and maintained in P2.

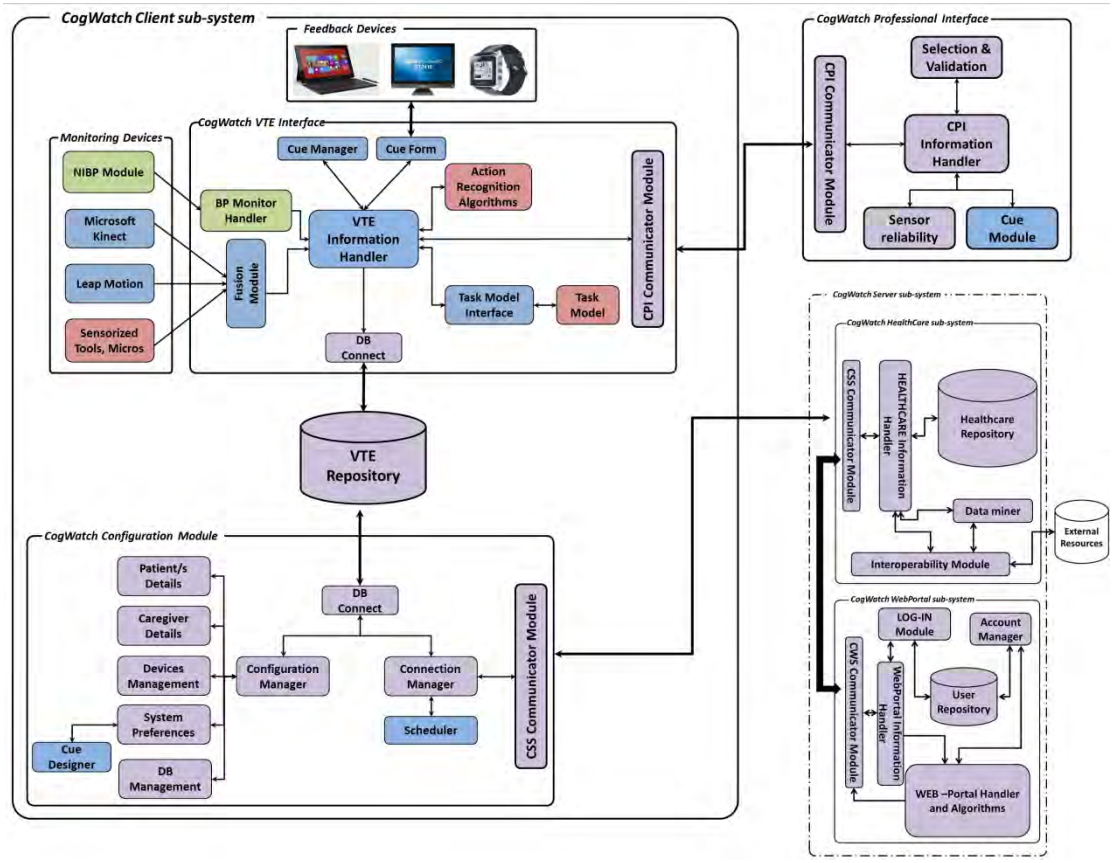

Figure 1 – CCS and CPI architecture of the CogWatch second prototype.

Figure 1 provides a schematic of the whole architecture proposed for the second prototype in terms of monitoring and feedback devices and software modules in the CCS and CPI sub-systems.

The CogWatch Client Subsystem (CCS) is implemented at home, and is focused on the collection and analysis of the data gathered during the rehabilitation sessions. The CCS is composed of different software modules designed and developed in order to provide special data link between the devices, manage the communication with database, communicate with the Action Recognition (AR) and Task Model (TM) modules and provide adequate feedback to the users.

The CogWatch Professional Interface (CPI) is the remote tool used to monitor and supervise the rehabilitation sessions. It allows clinicians to get information in real time about the performed actions, the committed errors and the reliability of the monitoring devices. Moreover the CPI will allow clinicians to correct and validate the results of the AR, in order to assure that the system will receive always the correct input.

Finally, the CogWatch Configuration Module manages the configuration properties of the CogWatch systems, as well as assures security aspects and the communication with the CogWatch Server sub-system.

3. COGWATCH CLIENT SUB-SYSTEM

In this section, a general overview of the CogWatch Client Subsystem is presented. All the software modules included in this part of the system are detailed in terms of functionality and interconnection with other components.

3.1 CogWatch VTE Interface

3.1.1 Blood Pressure Monitor Handler

See depicted scheme in figure below, for implemented solution.

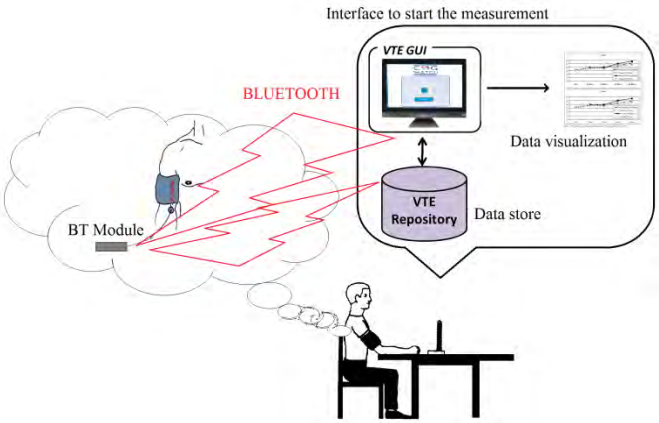

Figure 2 -Implemented solution.

The exchange of information between the sensors and the mobile application is based on a specific protocol called "TM EDS02".

The communication is established through a Bluetooth [1] module compatible with the standard 2.0 which emulates the behavior of an asynchronous serial channel. This module is classified as "class 1" so it provides a maximum range of 100 meters without obstacles.

The process used during a normal session to monitor the vital signs of the patient is as follows:

- The patient turns on the sensor module.
- After that, the sensor module activates Bluetooth permanently and the connection from the Gateway is established.
- The Gateway arranges the start of the session using the desired functioning mode.
- The sensor module transmits the corresponding information from the patient according to the mode selected.

- The session is considered as finished when the module is turned off or when the corresponding order to do that is sent from the Gateway.

The Gateway can manage certain aspects related to the performance of the module such as:

- ✓ Temporal suspension in the data transmission.
- ✓ Configuration of the information sent: samples of the signal and/or physiological measurements. When the module is turned on, the configuration by default is to send only the information related to the calculated measurements without the data from the signal samples.
- ✓ Remote turn off of the module.
- ✓ Specific controls related to the monitoring signal, i.e. filtering mode for ECG or mode of the measurement for PNI.

Exchanged messages

To establish the communication it is necessary to create a "start of session" process which consists basically of the exchange of information between the host and the sensor module for the configuration of the ID from the data frame. The process is as follows:

- Step 1: the host sends the corresponding command to start the session (0x43) to the sensor module. This frame includes the ID of the session assigned by the host and the transmission mode:

Comand:		0x43
ID:		0x00
Data:	NS	0x08
	MOD	0x0C
CKS:		0x29
FT:		0xFF

Figure 3 - Query to start the session.

- Step 2: the sensor module responses with the confirmation command (0x63) when it receives the query from the host. This new frame includes the ID of the type of module. The sensor module considers the session as initiated although no data is sent yet.

Comand:		0x63
ID:		0x00
Data:	NS	0x08
	TM	0x01
CKS:		0x14
FT:		0xFF

Figure 4 - Session started confirmation.

From then, all the necessary information to create the byte for the ID is available, both for the sensor module and the host. All the exchanged frames should then include the correct byte ID.

- Step 3: the host also considers the session initiated when it receives the confirmation from the module. It must also send back the control command of the active session with the value 0x02 in the byte ORDER, when it receives the information from the module and when it is ready to do that.

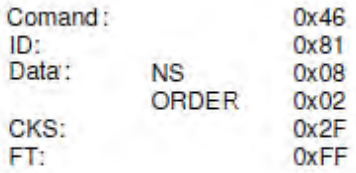

Figure 5 - Frame to finish the "start of session" process.

It is mandatory to send that frame to finish the "start of the session" process. After receiving this frame, the sensor module starts to send automatically the frames related to samples and measurements. From then, the sensor module sends the frames with the measurements and the host responses consequently, based on the frame received.

3.1.2 Fusion Module

As introduced in *"D2.3.1 Report in networks I",* this module is in charge to combine and synchronize the raw data gathered from the monitoring devices (described in *"D2.2.2 Report on devices II"*.). Figure 6 shows the block diagram proposed for the new FM, adapted to the new prototype. It maintains the original characteristics with respect to the previous version. Two new sensors have been introduced. The Leap sensors will gather information from the fingers and the toothbrush, while the Shimmer3 sensor will analyse the kinematic information of the dominant wrist used by the patient during the toothbrush session. Kinect™ will be used to track the face of the patient (instead of the hands as in prototype 1), providing important information of the approximation of the toothbrush to the mouth. For privacy reason, no videos will be recorded, since this task will be performed in the bathroom.

As show in Figure 6, The FM accepts as input:

- The information provided by Kinect™, focused on the position of relevant points around the face, in this case the mouth's points.
- The information provided by Leap, which is in charge of obtaining position of the representative points of the hand, such as palm centre or fingers, and from the tool grasped such as the toothbrush.
- Accelerations and forces from the coasters [18] attached to those objects to be manipulated, such as a glass of water.
- The data related to the behaviour of the patient's wrist, in terms or accelerations and orientations.

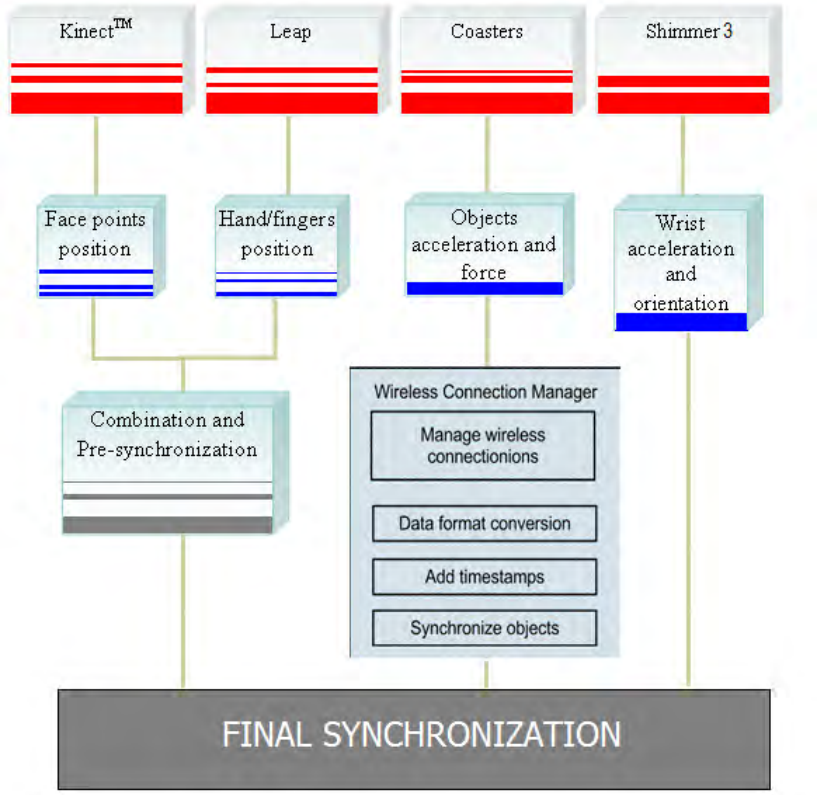

Figure 6 - Fusion Module block diagram.

The data provided by Kinect™ and Leap are combined and pre-synchronized in order to provide such data to the Fusion Module, so to consider the data source as a unique device.
The wireless connection manager, in the meantime, is principally focused on obtaining the data from the sensorized objects, which contain the coasters, through the Bluetooth communication, hence processing and synchronizing the information.
Finally, all data is synchronized and combined at the final stage with the data provided by the Shimmer3 sensor, in order to provide useful and reliable information to be used by the VTE Information Handler and to be sent to the corresponding algorithms for the action recognition and the error detection. The data is stored in a specific log files in the Data Base repository.

3.1.3 VTE Information Handler

According to the prototype architecture shown in Figure 1, the communication between the principal modules of the CogWatch Client Subsystem is based on a “star” typology, where the main control component is the VTE Information handler (IH). The IH module manages the communication with the following modules:

- Fusion Module, in charge of the data link from the monitoring devices.
- Action Recognition Algorithms and Task Model, focused on the recognition and the prediction of the action and the errors of the user.

- VTE Cue Manager, focused on managing the cues to prompt the user.
- Blood Pressure Module, in charge of providing data related to vital signs of patient, such as the heart rate and the blood pressure.
- Data Base repository. This module has a specific permission to exchange information with the Data Base Repository when required, especially, focused on the connection of devices and the relevant data of patient that may affect the performance of the cue prompting.

In addition, the IH is in charge of assigning priorities in order to protect the system from collapse due to overload. (*"D2.3.1 Report on networks I"*). This ensures the proper communication between the other software modules.

Considering the communication with the Fusion Module, the IH starts the connection with the monitoring devices and consequently the writing of the recording files that are stored in the Data Base once the session has terminated.

Then, the IH acts as a linker to send the raw data, derived from the Fusion Module, to the corresponding Action Recognition Algorithms. The output from these algorithms is successively sent to the Task Model to determine whether an error has been committed. The information about the error committed is obtained in terms of a specific code that allows the system to know what cue is needed, based on the information stored in the corresponding XML file.

The IH module gives the possibility of selecting the task (black tea, white tea, etc.) to be executed, in order to activate the Cue Form in which the corresponding cues are presented to the patient during the session. This new Form allows the patient to interact in real time with the module, as explained later in 3.1.5

Regarding the communication with the Blood Pressure Module, IH within VTE also activates a specific module to obtain the heart rate and blood pressure of the system when needed (currently, before and after the session).

Finally, this main software module provides direct access and continuing update of the Data Base in case of a setting change, even after a session is started.

3.1.4 Cue Manager

As previously described in *"D2.3.1 Report on networks I",* the CogWatch System holds different multimedia files used for providing different cues in the most suitable moment. This means that the system has to determine which is the most appropriate media file and locate it in the list of directories.

The Cue Manager (CM) is a new module in charge of localizing among the internal multimedia files the one most appropriate to show to the patient. Furthermore, there are different environmental constraints which the system must take into account. Constraints are set by the way in which the patient is used to perform an action. For this reason a number of different factors determine the behaviour of the system. These factors include:

- Time required for the patient to perform an action.
- The progress among the global task.
- Repeatability in the way of performing a task.

- User preferences.
- The way in which the information is shown to the patient.

The reason for including this extra module is to integrate the possibility of selecting from different tasks (i.e. prepare black tea, tooth brushing, etc.)

Below all the different cues included in the CogWatch system are listed:

- *Alarms*:

  Alert cues should always precede in time (.3sec) the informative cues, to direct attention to the screen to insure participants attend the information on the screen/speakers. The main objective is to make the patient aware of a wrong action without giving extra information.

  - Vibration: consist of a vibration of the watch.
  - Alarm sound: auditory beep.
- *Visual*:
  - Still: a static image displayed on screen for 10 s.
  - Videos: a video showing the performance of an action.
- *Auditory*:
  - Oral message: an oral message with an appropriate informative cue to the patient.
  - Ecological sound: an environmental sound which suggests an action to perform.
- *Written*:
  - Text message: a text message with the same information as the oral message.

The presented cues can be reproduced simultaneously or in sequence, depending on the clinician's selection.

The form of cue reproduction is conditioned by three main factors:

- *Language*: English, German or Spanish. (Current available languages)
- *Context*: the cue to be displayed depends on the sub-tasks already done by the patient. For example, if a patient has put the toothpaste on his toothbrush, the corresponding cue should display the toothbrush with the toothpaste, in order to identify exactly the sub-action.
- *Dominant hand*: actions can be shown from left/right handed perspective.

The CM module is in charge of identifying the different situations, in order to guarantee the selection of the correct cue taking into account the factors mentioned above. For achieving it, the CM relies on different information received from the Information Handler (IH) module, described in section 3.1.3, and depicted in Table 1.

Table 1 - Information managed by Cue Manager.

Information	Origin
Current error	TM
Next most probable action	TM
List of correct actions done	IH
Language	CCM
Dominant hand	CCM
Cue structure defined by the clinician	CCM

The module is based on different xml files for each of the possible kind of cues which stores the information necessary to reproduce the corresponding media. The output of this module is the structure of the cue to be displayed by the Cue Form. Nevertheless, the IH has to validate the priority of the cue and act as the final actor to decide when it is necessary to display a cue.

3.1.5 Cue Form

The Cue Form manages the interactions with the patient during a session, as described in previous deliverable *"D2.3.1 Report on networks I"*.

Interactions between the patient and the VTE interface are based on four buttons.

Three in-session buttons interact with the patient and an additional one is required for aborting the session at any time.

- The *"Quit"* button lets the patient abort the session at any time. When pressed, the session ends and the data recordings from to the session are deleted.
- In-session buttons:
  - *"Finish"* button: patient must press this button once he/she thinks the session has terminated.
  - *"Help"* button: by pressing this button the system will generate a new cue to assistance the patient.
  - *"Repeat"* button: by pressing this button the last cue (or combination of cues) displayed is shown again.

Additionally, Cue Form provides different layouts to define some additional cues to measure general progress during the performing of a task. These cues are:

- *Cue Progress*: a portrait view of the correct sub-actions done by the patient represented by a still.

- *Cue Goal*: a still of the final state of the task to remind the session objective to the patient.

3.1.6 Action Recognition Algorithms

The current CogWatch Action Recognition (AR) system is described in detail in deliverable D3.2.2 “Report on data analysis for Action Recognition II”. Consequently only a brief summary is presented here.

AR in CogWatch follows a statistical pattern recognition approach based on Hidden Markov Models (HMMs) [6-8]. Because actions can occur simultaneously, or at least in overlapping time, and not necessarily in a well-ordered sequence, a conventional HMM based system is inappropriate. Instead CogWatch uses a novel architecture based on a parallel set of sub-goal detectors (a sub-goal is one of the basic actions into which a task is broken using a method called Hierarchical Task Analysis; in the “tea-making” task that is the basis of CogWatch prototype 1 an example of a sub-goal is “add milk”). Each detector is a stand-alone HMM-based pattern recognition system (called a Viterbi decoder) that is responsible for detecting an instance of a given sub-goal. A detector takes inputs from the set of sensors that are attached to the objects that are involved in its sub-goal or are otherwise relevant to the sub-goal.

The real-time CogWatch AR is implemented in C#. In order to run indefinitely in real time, each detector uses a technique called “partial trace-back”. This allows the detectors’ explanations of the sensor data to be output, and the corresponding memory to be released, as soon as they become unambiguous.

AR based on instrumented objects (cups, mugs, kettles fitted with the CogWatch Instrumented Coaster (CIC) has proved to be extremely reliable. Indeed, in the most recent experiments, errors have only occurred when there are faults in the sensor outputs (for example, due to a Bluetooth communication fault). Problems with delays in the output of the AR (“latency”) due to ambiguity in the detectors’ interpretations of the sensor data have also been resolved, so that the current AR in prototype 1 runs with negligible latency.

It is important to realise that the CogWatch real-time AR system is generic and not restricted to any particular application. Given a hierarchical analysis of a task and sufficient examples of sensor data for the sub-goals of that task, a set of sub-goal HMMs can be built using a standard “off-the-shelf” toolkit (called HTK) [19]. These HMMs can then be loaded directly into the CogWatch AR.

3.1.7 Task Model Interface

The Task Model Interface (TMI) module is in charge of supervising connections between the Task Model and the Information Handler. Task Model exchanges messages with the Information Handler through a local socket, see Figure 7. The management of this connection is controlled by the Task Model Interface. Additionally, this module can be used to simulate the behaviour of the Task Model.

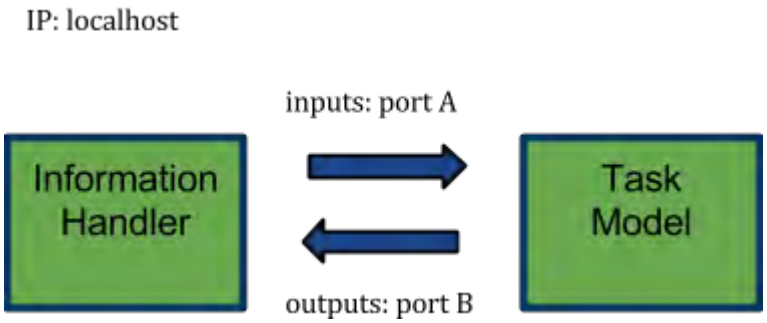

Figure 7 - TMI workflow.

The information exchanged is summarized in the following table:

Table 2 - Information exchanged between TM and IH.

Information	From	To
Current error	TM	IH
Next most probable action	TM	IH
List of correct actions done	TM	IH
Favourite sequence	IH	TM
Interaction with buttons	IH	TM
Current action performed by the patient	IH	TM

The module generates events which are handled by the IH according to their priority.

3.1.8 Task Model

The CogWatch Task Model (TM) is described in detail in deliverable *D3.3.2 "Report on Predictive Models II"*, and only a brief description is included here.

The basic TM, incorporated into prototype 1, is based on a Markov Decision Process (MDP). An MDP is a simple statistical model consisting of:

- A set S of states,
- A set A of actions,
- For each pair of states s_1 and s_2 and action a,
  - a transition probability $P_a(s_1,s_2)$ which is the probability of moving from state s_1 to s_2 given that action a has been performed, and
  - a corresponding cost $C_a(s_1,s_2)$.

For example, in the case of the tea-making task, the actions *A* are the sub-goals of tea-making performed by the patient, and the states are sequences of sub-goals that can be extended to result in successful task completion.

At each point during the task the TM will be in a state, s_1 say. When the patient executes a sub-goal the TM receives an action *a* from the AR system. If adding *a* to the state s_1 results in another valid state s_2, then $P_a(s_1,s_2) = 1$ and the system moves to state s_2. However, if s2 is not a valid state then an error has occurred and it may be necessary to prompt or cue the patient.

The prompt or cue is informed by the MDP's *optimal strategy*. A *strategy* is just a function π that associates each state *s* of the MDP with an action $\pi(s)$. The optimal strategy is the strategy that minimises the expected cost of completing the task. In other words, if a patient has reached state *s* and wishes to complete the task with minimum cost, then the patient should execute the action $\pi(s)$. The optimal strategy is pre-computed in advance, before the system is deployed.

Clearly the optimal strategy will depend on the cost function *C*. The most effective cost functions are those that reflect the priorities of the clinicians who are working with the patients. This is discussed in D3.3.2.

One of the problems associated with an MDP-based Task Model is that it is ill-equipped to cope with any errors that are made by the AR. The MDP-based TM "believes" the outputs from the AR and moves between states accordingly. If the AR makes an error the state of the TM will no longer correspond to the stage of the task that the patient has reached.

A solution to this problem is to replace the MDP with a POMDP - a Partially Observable Markov Decision Process. In a POMDP the concept of state is replaced by that of a "belief state". A belief state is a probability distribution over the states of the underlying MDP. By combining this mechanism with a probabilistic model of the errors that are likely to be made by the AR, a TM can be developed that is more robust to AR errors [.

Experiments demonstrating the superior performance of a POMDP-based Task Model have been conducted and are reported in D3.3.2.

3.1.9 DB Connect

The *DB Connect* is the module that manages the connection and all the queries with the *VTE Local Repository*. The module has been created with the objective of centralising the database connection for better management of the data interchanges.

The *DB Connect* module provides methods for managing the *VTE Local Repository* structure. The methods can be grouped based on their responsibility: connect, create (insert), edit (update), select or delete (drop) database elements.

Figure 8 shows the workflow of the *DB Connect* manager in CogWatch during the write and read process. In particular, it is important to highlight that the different methods are reusable.

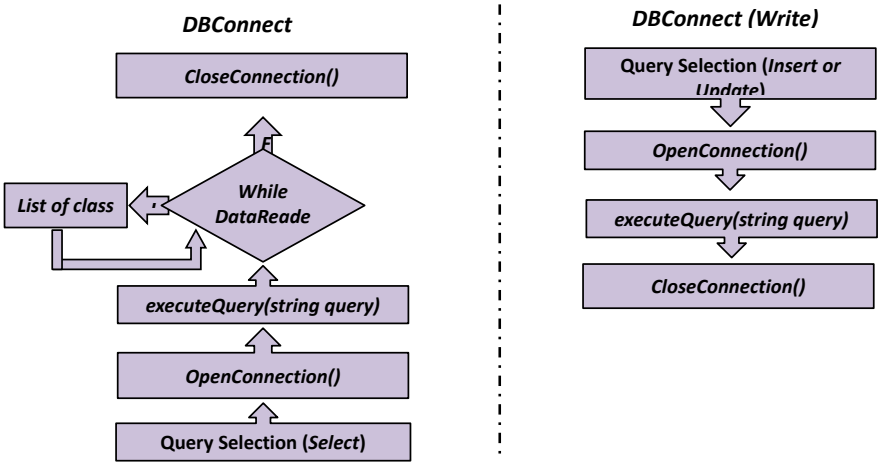

Figure 8 - *DB Connect workflow*

The *open* and *close* methods, used for the connection with the local DB, are *private methods*, in order to **guarantee** that the DB is accessed only from the manager, and it is correctly opened and closed. Generally speaking a "*private method"* cannot be called from outside its class. It can be called only from other class methods—this promotes information hiding. Programs become easier to maintain and test.

3.1.10 CPI Communicator module

The *CPI Communicator Module* is responsible for establishing and transferring information with the corresponding communicator module located in the *CogWatch Professional Interface* (CPI) (see section 4).

Table 3 - Communication messages between VTE and CPI

Header	*Message example*	Action	Direction
A	*"A-T0001"*	Task Model Selection	VTE->CPI
B	*"B-PTUPM001#Lucio Martin Usera"*	Patient Information	VTE->CPI
D	*"D#no_alarm#no_visual#N#verbal#MEDIA/VERB/Audio_cues/Cues for sub-action/EN/A4_cue_Add_boiled_water_in_cup.wav#True#Please, add water to the cup.#False#E01#A4"*	Task Model Information	VTE->CPI
E	*"E1-OB01- Kettle Base true"*	Sensors Reliability	VTE->CPI
F	*"F-2014-04-15 11:57:07"*	Session Start	VTE->CPI
G	*"G-2014-04-15 11:58:49"*	Finish time	VTE->CPI

H	*"H#FinishSession"*	End of Session	VTE->CPI
I	*"I#30"*	Reset perplexity timer	VTE->CPI
T	*"T#A7" (Stir)*	AR Results	VTE->CPI
Z	*"Z-Closing"*	Close all / disconnect	VTE->CPI
E	*"E-A8:remove tea bag"*	Validated Action	CPI->VTE
N	*"N"*	Next Cue	CPI->VTE
R	*"R"*	Reset Counter	CPI->VTE

The communication between the CPI and VTE is based on a socket network technology. In particular, a *Raw IP socket* is established when a new session starts. In a connection-oriented client-to-server model, the socket on the server process waits for requests from a client. To do this, the server first establishes (binds) an address that clients can use to find the server. When the address is established, the server waits for clients to request a service. The server performs the client's request and sends the reply back to the client. The two endpoints establish a connection, and bring the client and server together. The client-to-server data exchange takes place when a client connects to the server through a socket. In the CogWatch system, the VTE is defined as client while the CPI is the server.

The main function of this module is to interchange codified messages and translate them in precise command by the dedicated module. Table 3 shows the different codified messages that are exchanged between the VTE and the CPI. Every message is composed by the header, that identifies a unique information message, and a body message, that contains the information related to the action.

The Task Model codified message (*D*) contains 10 elements, specifying all the details about the defined action, the task model and the selected cue. In particular:

1. Type of Alarm : no alarm/ watch vibration / acoustic [beep]. Possible values: no alarm/vib/beep.
2. Type of visual cue. Possible values: no visual/still/video.
3. Path for the visual cue("N" if no visual cue).
4. Type of auditory cue. Possible values: no auditory/eco/verbal.
5. Path for the auditory cue("N" if no auditory cue).
6. Indicate if the text cue is showed or not. Possible values: True/False.
7. Text of the text alarm.("N" if no text).
8. Type of feedback. Possible value: True/False. In case of "True", the Path_A and Text_A will be selected.
9. Error Code.
10. Activity Code.

In order to ensure security, a Rijndael Encryption algorithm [10] is applied to the message before sending it. See Section 5.4 for more information about the security algorithms used. Some examples are presented below:

Patient information message before encryption:

```
B- PTUPM001#Lucio Martin Usera
```

Patient information after encryption:

```
li2dPbT22Z9X0Male1Bzv6R8iSk+4KrRjhUa+fRYv6U=
```

Task Model message before encryption:

```
D#no_alarm#no_visual#N#verbal#MEDIA/VERB/Audio_cues/Cues for sub-action/EN/A4_cue_Add_boiled_water_in_cup.wav#True#Please, add water to the cup.#False#E01#A4
```

Task Model message after encryption:

```
Q+Yrs3h8mVXv7EbfZ6++KWpLsB6lsZNws5S8Iyg9ZbjaMITR5kUXoG38OB8l6X7Ut/fvSLju8EW8TFTMSnLRWuKzVzKix8+XTRnRiMz9mJA388VnBHFBIaOCgNewvWi8vBu7yAm08GOPJqz6U7Wm5Swxdra4aoenMM75QcnqeDOA+Uux6zJgRNb0pMMP4E2eMsuIMaNQGVKYWOMjsrYaJA==
```

3.2 VTE Local Repository

The VTE Repository is to manage generic but essential information about the users of the CogWatch System and the data coming from the scheduled rehabilitation sessions. The *VTE Local Repository* has not been subject to modification. The description can be found in *"D2.3.1 Report on networks I".*

3.3 CogWatch Configuration module

3.3.1 DB Connect

The *DB Connect* module included in the CogWatch Configuration Module has the same functionalities described in section 3.1.9 of this document.

3.3.2 Configuration Manager

The configuration manager has been created to allow the configuration of the CogWatch system locally. A CW specialist (usually an account manager or a technician) can directly select from the taskbar the CW icon and choose the setting button, as show in Figure 9.

Figure 9 – CW button on TaskBar

The access to the configuration manager is controlled by an authenticated process, to allow only authorized personnel to log-in.

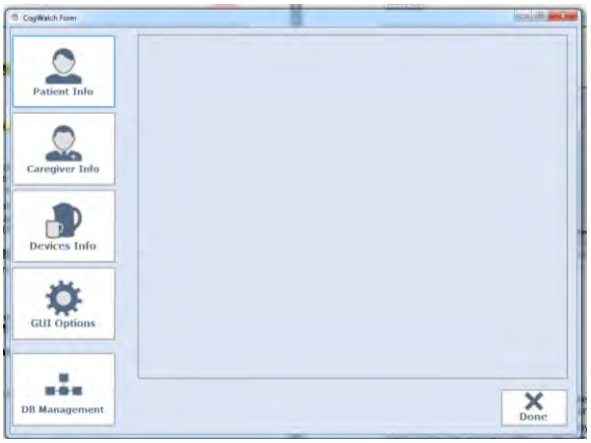

Figure 10 - Configuration Manager after LogIn

In particular, through the Configuration Manager, it is possible to:

1. *Manage Patients details*

Figure 11 – Patient Form

2. *Manage Caregiver details*

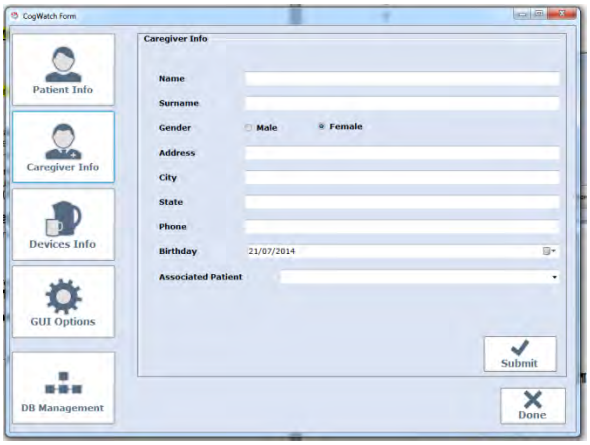

Figure 12 - Caregiver Form

3. *Configure the devices information*

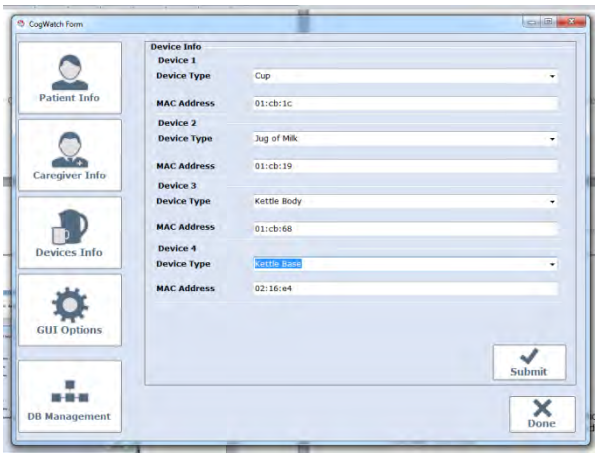

Figure 13 - Device Form

4. *Configure the VTE GUI options*

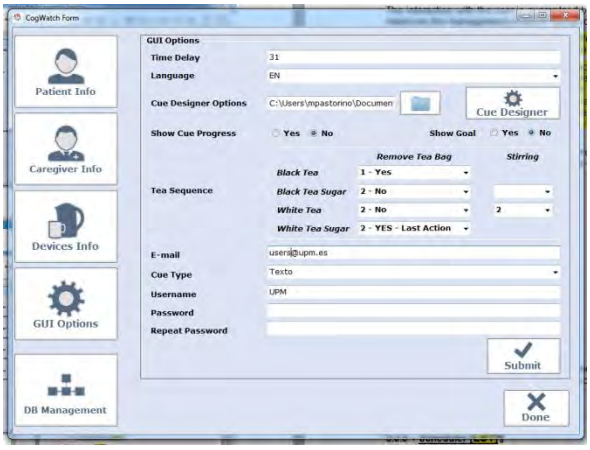

Figure 14 - GUI Form

5. *Manage the local VTE Local Repository [3.2]*

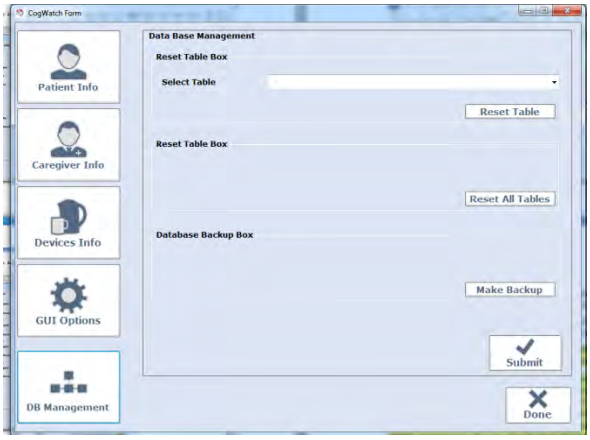

Figure 15 - DB Manager Form

Once selected and validated, the information is stored in the ***VTE Local Repository***, using the ***DB Connect*** [Section 3.1.9] module

3.3.3 Cue Designer

The *Cue Designer* aims to provide a simple tool to clinicians allowing them to create a personalized error feedback table or modify an existing one.

The Cue Designer aims to provide a simple way for managing the interaction with clinicians when modifying a personalized error feedback table or even more, when creating a new one.

This application has been implemented to enable the clinician defining his/her own error feedback definitions and, ultimately, his/her own error table. To that end the application gives as an output a configuration file required by the CogWatch VTE Interface for managing the cue system. The principal novelty is that the clinician can save and load different error feedback configuration files and modify the way in which the system prompts cues to adapt it to the most relevant for the patient.

As in other CogWatch' applications, accessibility is guaranteed by setting different languages and layouts.

The main screen is composed by the error feedback table which the user can modify by editing the different fields, see Figure 16.

Figure 16 - Cue Designer Module: main screen.

Once the table is opened, the module lets the user modify several features such as the description of the error or type of error, when the user wants the application to restart a cue sequence and also design these sequences.

The structure of the cue prompting is composed by cues, which are the information shown to the patient each time she/he commits an error. In a lower level, each cue is composed by a sequence of states, which are any combination of cues displayed at the same time. The application allows the user to define up to 12 cues composed by up to 6 states.

According to this definition the clinician can add new states in terms of new kind of cues which are classified as:

- *Alarms*:
  - Vibrations.
  - Acoustics.
- *Visual*:
  - Images.
  - Videos.
- *Audio*:
  - Verbal message.
  - Ecological sound.
- *Written*:
  - Text message.

From the cue designer form, see Figure 17, the user can modify each of the defined cues created previously, also, the user can modify at the same time the cues of more than one error as a time, which could be useful in case the user want to define a subset of errors which requires the same feedback structure.

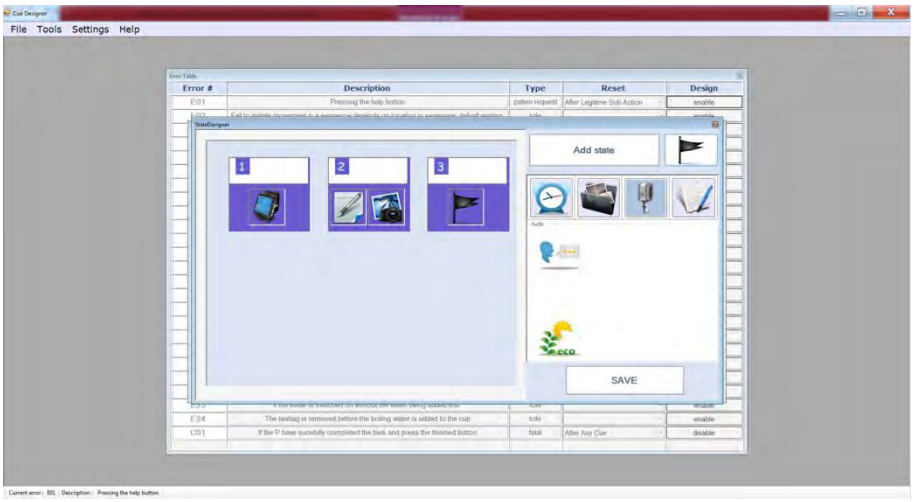

Figure 17 - Cue designer form.

The following restriction and consideration has been taken into account for the design of the application and are intrinsically imposed on the user:

Restrictions:

- Video or stills can be chosen, not both
- Verbal auditory instructions or ecological sounds can be chosen, not both

Something to note:

- Alert cues should always precede in time (3 sec) the informative cues, to direct attention to the screen to ensure participants attend the information on the screen/speakers.

- Still & written cues stay on the screen for 10 sec or until any sub-task is completed. The cues should appear with no animation.
- Video & auditory cues should be played once. Though this can be repeated using the 'repeat' button.
- All cues are informative now, so even if the patients perseverate – the system will cue them with the next best action (except errors E07, E12 or when cueing follows 1c – alert for errors). This is indicated in the table as follow E01, note E01 is fatal after 3 occurrences; however counting is set to zero after a legitimate sub-task is carried out. In other words if TM has identified an error, the counting should not be re-set. It is assumed that you receive information directly from the AR/clinician button on what is happening otherwise.

When the user finishes the new design or modification of an existing error feedback table, the module manages the storage of the new data to be used during the session via the "Cue Manager" (3.1.4).

3.3.4 Connection Manager

The CCM connection manager is the module in charge of managing the connection to and from the CogWatch server subsystem (CSS). Depending on the information coming from the DB connect, it will responsible for routing them to the ***Scheduler*** or to the ***CSS Communication Module***.

3.3.5 Scheduler

The CCM Scheduler is the module in charge of the scheduling management. It will launch a new rehabilitation session and save the details of a new scheduled session in the VTE local repository.

This Module will always be working while the system is in idle mode. The Scheduler will be checking continuously the following upcoming task in the time table while the system is idle. The time table will be set by an ad hoc interface in the CW configuration module and by a web form in the Web portal. The Scheduler is not allowed to retrieve data directly from the data base; it will use the DB Connect module. Only the clinicians and therapists are allowed to schedule the rehabilitation sessions, using the tools provided by the CogWatch system.

3.3.6 CSS Communicator Module

The CSS Communicator Module is responsible to establish and transfer the information between the CCS and CSS.

The expected data from the CCS are the results and statistics of the performed rehabilitation sessions while, for the expected data from the CSS, these concern new scheduled sessions of the rehabilitation session. The communication between the two components is bidirectional and it is independent of the channel's nature as well as the protocols used in the low levels of the network stack.

Finally, in order to handle large amount of data and avoid high traffic situations, the Communicator Module compression algorithms are used to limit the size of the data exchanged. Moreover, an encryption mechanism is implemented in order to secure the channel from malicious attacks using both symmetric and asymmetric encryption.

In order to establish this kind of connection between the communicators, two objects have been created, one for the CCS and one for the CSS respectively. The architecture of the Communicator Module is presented in Figure 18.

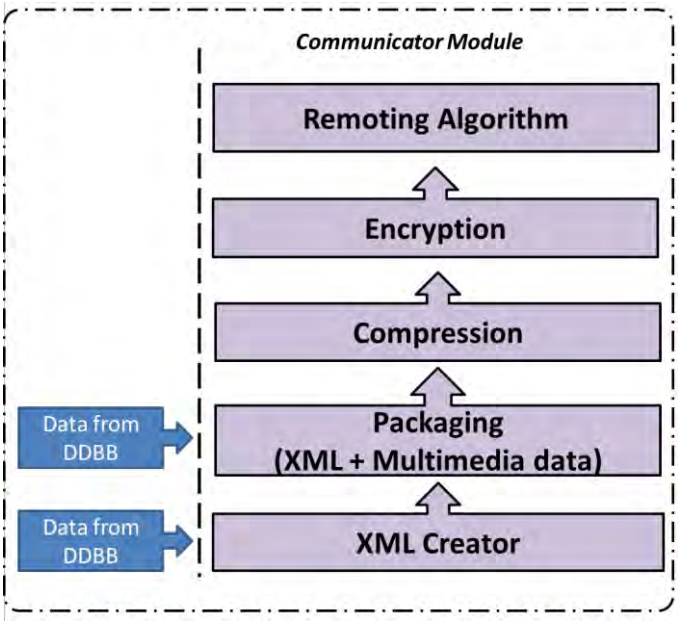

Figure 18 - Communicator Module of CCS

When the CCS wants to update data from the CHS, it calls the objects of the CHS unit. Similarly, when the CHS wants to update data from the CCS it calls the CCS object. The Https Channel class is the preferred class to be used for the communication channel, as it provides support for wire-level protection using Secure Sockets Layer (SSL) and authentication using Integrated Windows Authentication or Kerberos, more details about security and protocols are described in section 5.4.

4. COGWATCH PROFESSIONAL INTERFACE

The CogWatch Professional Interface (CPI) is the remote clinician platform used by the professional to supervise the rehabilitation sessions. The interface allows the professionals involved in the rehabilitation process to control the action executed by the patient in real-time.

Figure 19 shows the main view of the CPI with several data streams that indicate to the professional the state of the current rehabilitation session.

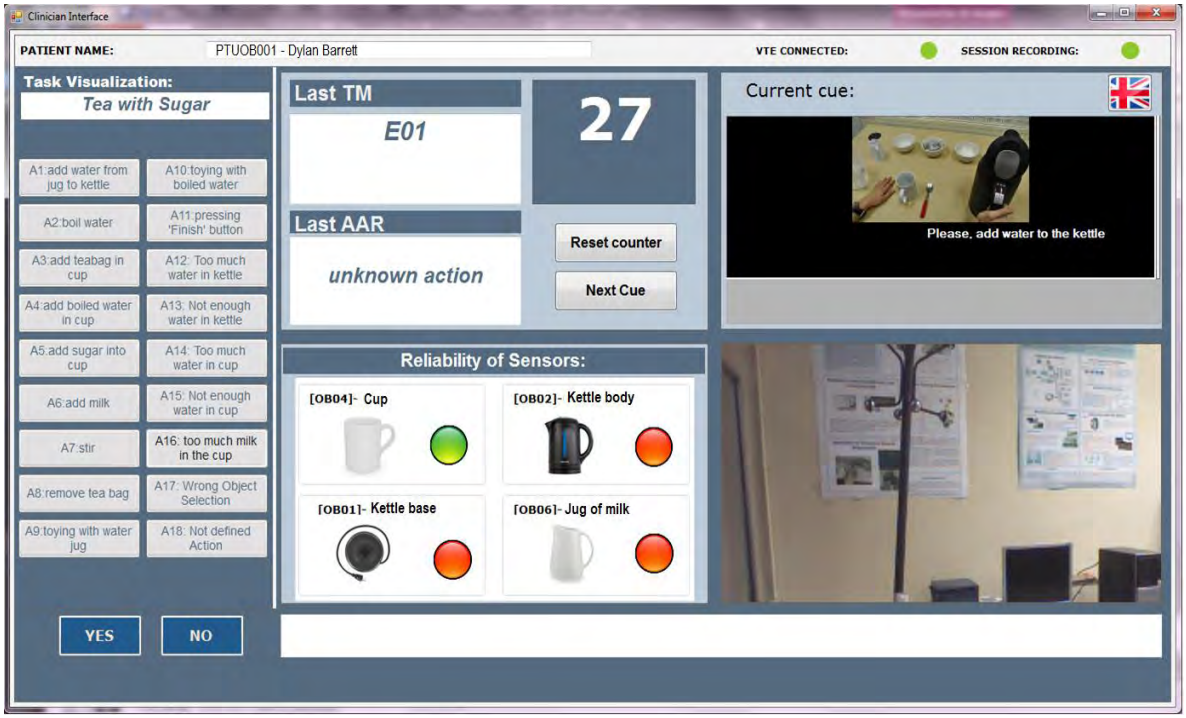

Figure 19 - Main view of the CogWatch Professional Interface

Two typologies of rehabilitation session are possible:

- *Preparing a tea*: the patient selects, from the VTE interface, the intention to carry out a tea task session. Then the patient chooses among four different kinds of teas: tea with sugar, tea with sugar and milk, black tea with sugar, black tea with sugar and milk. Once the patient makes the selection, the session starts in both the VTE and the CPI interfaces.
- *Brushing the teeth*: the patient selects the action of brushing the teeth. Then the session starts to be recorded in both the VTE and the CPI interfaces.

The information in the main screen, for both the tasks, is represented as following:

Patient profile information: the patient ID number and name, showed in the upper-left side of the screen. This information appears as a VTE connection is established

VTE Connection and Session recording light emitting diodes (LEDs): The CPI interface can work in background, waiting for new rehabilitation sessions. When a VTE-CPI connection is

established, the VTE CONNECTED LED changes from red to green. This means that the patient has opened the VTE to start a new session.

Then the patient chooses the type of rehabilitation session, that is to prepare a cup of tea or to brush the teeth. As the start session button of VTE is pressed, the SESSION RECORDING LED of CPI become green and the CPI starts to record the session.

Task Visualization and Sub-Task buttons: A window box, placed in the right side of the screen, indicates the type of task to be executed. According to the task, a set of buttons are shown, each one associated to a specific sub-task.

Task Model (TM) and Automatic Action Recognition (AAR) information box: the central part of the screen is focused on the sub-task execution and on the information coming from the recognition algorithm. The TM and AAR box includes the following information:

- Last TM: show the last error performed by the patient and detected by the Task Model
- Last AAR: show the last sub-action performed by the patient and detected by the Action Recognition algorithm
- Countdown timer: this timer, set by the professional in the Configuration Setting, defines the time, in seconds, within which a sub-action must be performed by the patient. When the time expires, a cue, with the related sub-action, is sent to the patient.
- Reset counter button: used to reset the timer in case the physician wants to give more time to the patient during a specific sub-action.
- Next Cue button: used to send the cue to a specific sub-action before waiting for the ending of the timer

Cue Box: this box, placed in the upper-right side of the screen, shows the video of the current cue sent to the patient. Moreover, a button with an icon flag is present to allow the professional to set the language of the cue in English, Dutch or Spanish.

Video Box: the video box, placed in the lower-right side of the screen, shows the video of the rehabilitation session executed in real-time by the patient. The video is recorded from the Microsoft Kinect, connected to the VTE. The camera is positioned to record the actions executed by the patient over the table surface while keeping his or her identity anonymous.

Reliability of Sensors: this box, placed in the lower centre portion of the screen, shows the reliability of the sensors positioned on the tools used by the patient during the rehabilitation session. The sensors, in fact, should record data during all the session and send the information via Bluetooth to the VTE. The status of each sensor is indicated by a LED. When a sensor is on, the related LED is coloured in green. When the sensor is off, the related LED is coloured in *red.*

Confirmation label: when a sub-task button is pressed, the selection must be confirmed through a confirmation label, situated in the lower part of the screen. The professional can press the YES button to confirm the selection or the NO to reset the selection.

4.1.1 CPI Communicator Module

The CPI Communicator Module, already introduced in the CogWatch Client Sub-System (3.1.10) is responsible for establishing and transferring the information with the communicator module located in the CogWatch VTE Interface (VTE). The communicator module, the relative functions and the encryption methods for data transmission and communication, are described in paragraph 3.1.9.

4.1.2 Selection & Validation

The selection and validation module is in charge of validating the algorithms coming from the VTE. The validation is executed by the professional during the rehabilitation session. The professional observes the subtask or the error detected by the AAR and showed in the TM and AAR box. Four different circumstances can be presented

- *The information showed in the TM and AAR box is correct*: the professional can confirm it through the YES button.
- The information showed in the TM and AAR box is not correct: the professional can change the selection by resetting it through the NO button and then select the proper subtask button and confirm it through the YES button.
- No information is showed in the *TM and AAR box*: the professional selected the proposed sub-task button and confirms it through the YES button.
- Unexpected information is shown: information is showed in TM and AAR box but no action has been executed by the patient. In this case, the professional must reset the information through the NO button.

4.1.3 CPI Information Handler

The CPI information handler is responsible to receive and direct the data coming from the VTE. When an information data arrives from the VTE to the CPI, it is decrypted by the communication module. After this first step, the decrypted information is named by specific codification. The Information Handler is responsible to encode the data and redirect it to the appropriate module.

4.1.4 Sensor reliability

This module is responsible to check the sensor reliability. As described in the introduction, the reliability of the sensors is showed in a specific box. The sensors, placed in the tools, must record the data during the rehabilitation session. Then the recording data are sent via Bluetooth and stored to the VTE.

The status of each sensor is indicated by a LED. When a sensor is on, the related LED is coloured in green. When the sensor is off, the related LED is coloured in red.

4.1.5 Cue Module

The Cue Module is responsible to detect the cues showed in the VTE interface and reproduces them in the Cue Box. The cues are managed by the Cue Manager, described in paragraph 3.1.4.

5. COGWATCH SERVER SUB-SYSTEM

The CogWatch Server sub-system (CSS) is dedicated to the storage and visualization process of all patient data and rehabilitation sessions statistics. It is designed to assist the clinician in the follow-up of the patient rehabilitation of AADS. As described in *"D2.3.1 Report on networks I"* the CSS is composed by two different modules, the *CogWatch HealthCare sub-system* (CHS) and the *CogWatch WebPortal sub-system* (CWS). Detailed information about the CHS and CWS are presented in the following sections.

5.1 CogWatch HealthCare sub-system

The *CogWatch HealthCare sub-system* (*CHS*) is defined as the remote healthcare server, in charge of communication with the *CCS* and receiving from it data and statistics of rehabilitation sessions. The *CHS* is dedicated to the storage of the medical and personal information of the patient's assigned to each Healthcare centre.

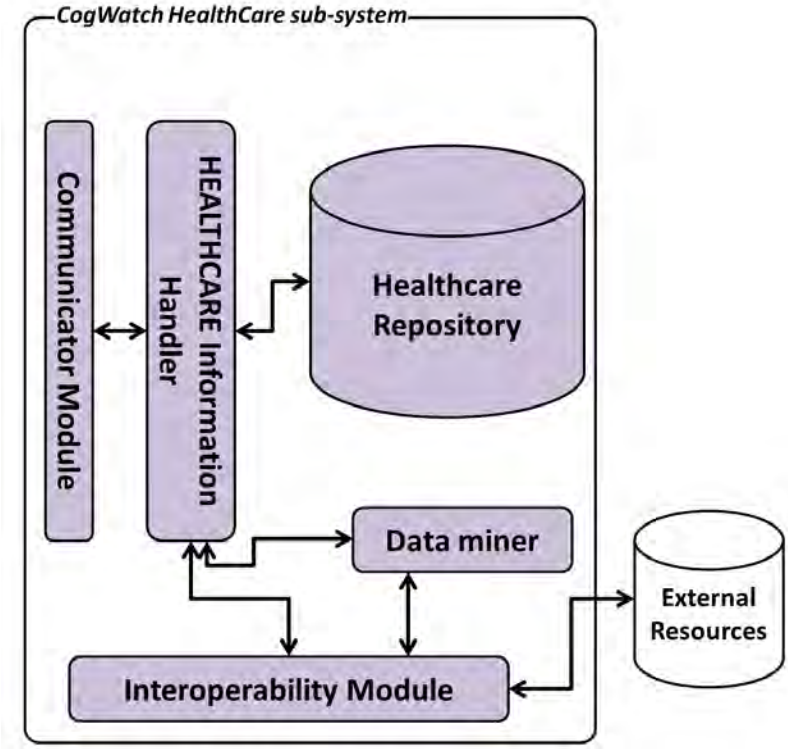

Figure 20 - CogWatch HealthCare sub-system

The ***CHS*** structure has not been changed with respect to the architecture of the CogWatch first prototype. For detailed information please refer to *"D2.3.1 Report on networks I"*.

5.2 CogWatch WebPortal sub-system

The *Web Portal Sub-system* (CWS), Figure 21, is dedicated to the allocation of the medical web portal and the account information repository. This will be an independent and unique server.

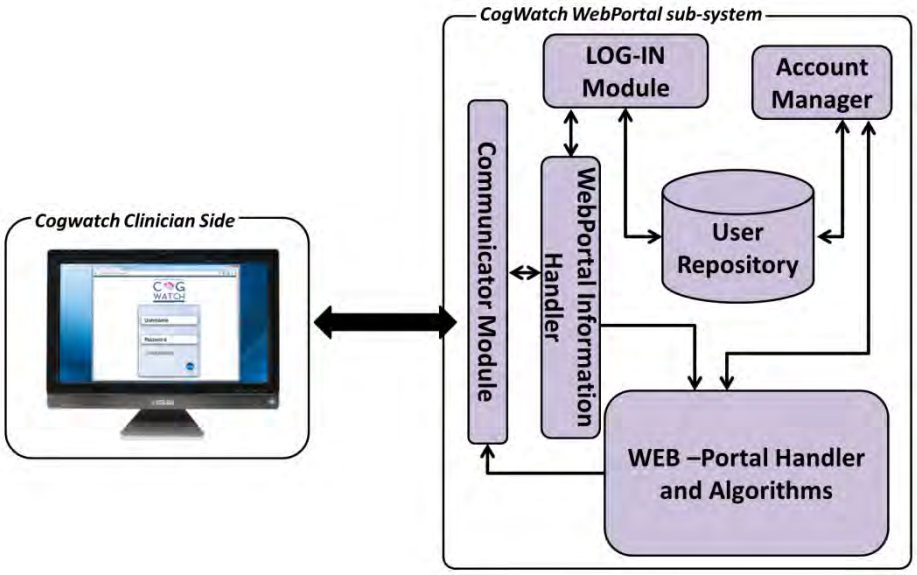

Figure 21 - CogWatch WebPortal sub-system

The *CWS* structure has not been changed with respect to the architecture of the CogWatch first prototype. For detailed information please refer to *"D2.3.1 Report on networks I"*.

5.3 Security and Privacy layer

Security and privacy aspects represent a paramount priority for the CogWatch system, especially in the case of patient privacy. The description of such issues, already presented in the deliverable D1.3.1 for prototype P1, are reported within this paragraph in order to integrate and upgrade the network and communication's requirements to the prototype P2. The main issues related to these aspects include physical security, database and web security, access controls, user authentication, data encryption/decryption and data secure transmission.

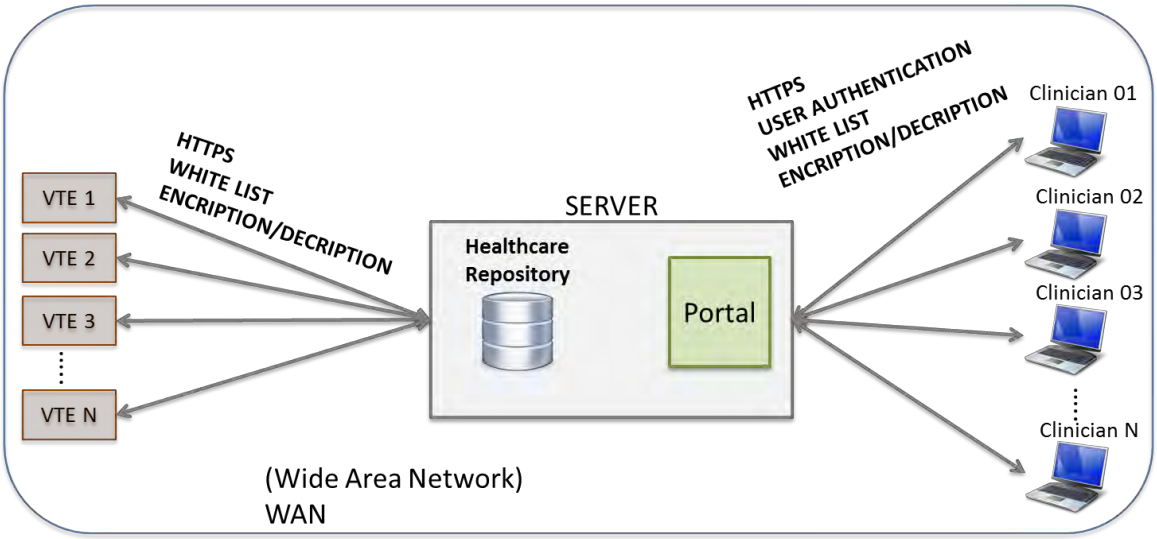

Figure 22 - CogWatch Network and Security protocols

Fig 24 depicts the relation between the CSS and multiple sub-systems each supporting one VTE on the one hand and multiple CPIs on the other. The platform has been developed with the aim of ensuring reliability, privacy and confidentiality of the data. This objective includes the following practices:

- *Risk management of the system*: The risks of use of the platform have been deeply analysed according to the guidelines provided from the literature. Different set of tests have been performed to each component before the prototype trials, in order to guarantee the effectiveness of the risk management protocols.
- *Traceability of components*: each component must have a serial number and a record to be used for traceability's management.
- *User and Installation manuals*: each component will have a user manual and an installation manual.
- *Communications security*: PC-client – PC-server: In P1.1 the communication between patient and clinician interfaces is only local. This means that the different modules of the system are connected through an internal LAN network with no access to internet. Consequently no hacking activities from external sources are possible.
- *Data Storage*:
    - Patients' data are stored locally in the VTE system database.
    - Data are stored through an anonymous format.
    - The data are stored in a database MySQL Server that offer different security features as:
        - Data integrity
        - Data recovery
        - Database backup

- Only the system administrator has the authority to access to the MySQL data, through a password.

- *User privacy*:
  - All user data are gathering through anonymous format. Users are identified with only ID number.
  - All data are stored locally in the VTE system
  - The video data of the rehabilitation session are anonymized though and avataring process

Finally, CogWatch prototype P2 will adopt a more distributed and complex architecture than CogWatch prototype P1: in fact, patient and clinician system will be connected through a WAN network, via internet.

5.4 Security

The development of a cognitive rehabilitation system based on wireless communications (BAN, LAN, WAN) may offers lots of advantages and novel challenges, such as reliable data transmission, mobility support, fast event detection and timely delivery of data. Unfortunately, technologies in healthcare systems can make users privacy vulnerable if security aspects are not considered. With respect to CogWatch system, the patient's activity monitoring, behaviour data and physiological vital signals are very sensitive. These data are daily shared between patients and professionals through the VTE and the CPI interfaces. A potential unauthorized collection and use of patient data by potential adversaries can cause life-threatening risks to the patient, or make the patient's private matters publically available. Thus the patient security and privacy is the central concern in the CogWatch system. The following sub-sections explore the security aspects and the consequent developed strategies considered within the CogWatch system. The technical solutions that have been employed ensure a high level of security, avoiding potential threats that can endanger the patients or the professionals` applications.

Both the communication VTE-SERVER and the communication SERVER-CLINICIAN INTERFACE will adopt the following transmission security features:

- Microsoft .NET Framework cryptographic services, for encryption and decryption of all data, to secure encoding and decoding of data [5, 22].
- Hypertext Transfer Protocol Secure (HTTPS). HTTPS provides authentication of the web site and associated web server that one is communicating with, which protects against different attacks as the example of the man-in-the-middle.

White list through IP filtering to allow the communication and transmission of data only between the IP addresses listed, avoiding the connection of other users. Only the Administrator can access and modify the list of allowed IP addresses

5.4.1 CogWatch Security Architecture

Figure 23 depicts the CogWatch system, showing the communication among the different modules and the security aspects to be addressed.

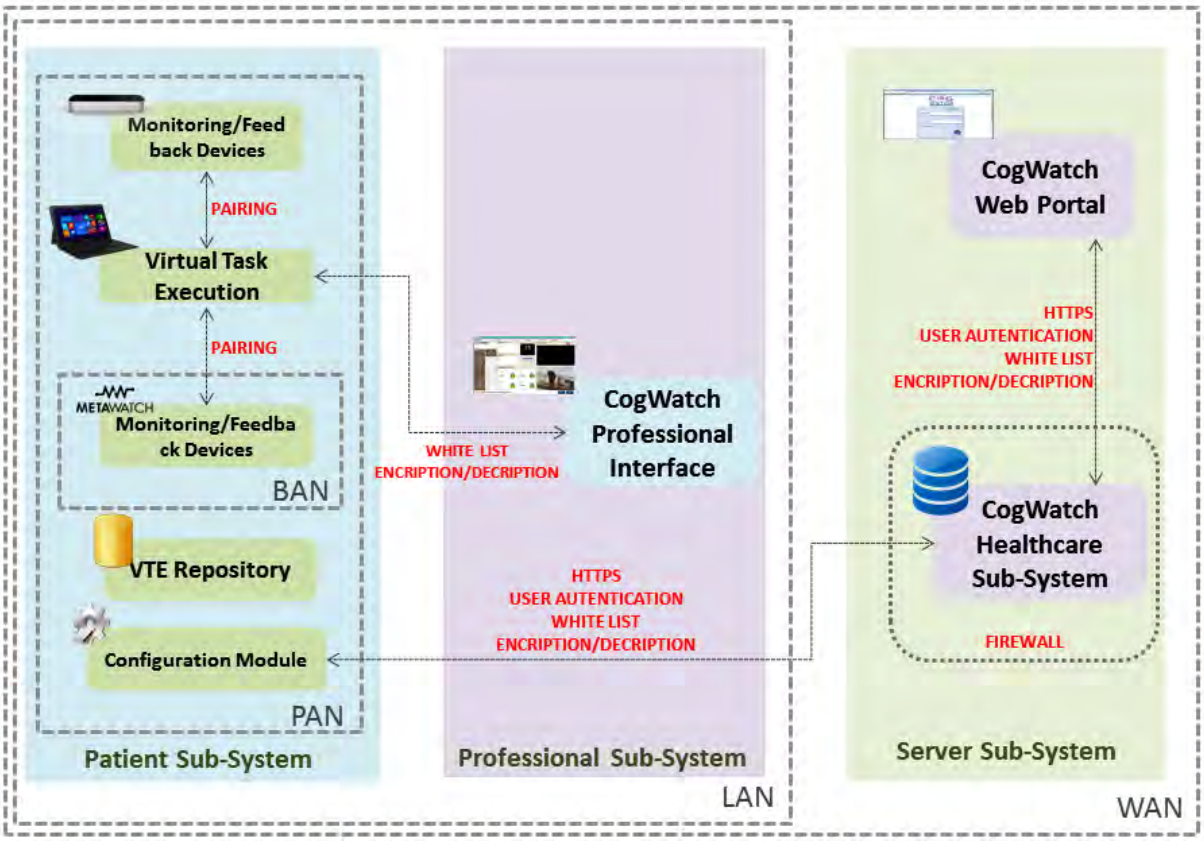

Figure 23 - CogWatch Networks and related security protocols

The platform is set up by three sub-systems: Patient Sub-System, Professional Sub-System and Server Sub-System. The security architecture aspects have been defined to manage the privacy and security issues with respect to the network and the communication among the sub-systems as the modules within them.

The networks and the related types of security services are described in the next sections.

Body Area Network (BAN): this network is set up by a system of devices in close proximity to a person's body that cooperate for the benefit of the user. With respect to the CogWatch system, a BAN network has been identified with the sub-group of the monitoring and the feedback devices that are physically wear or joined to the patient (see D2.3.1 for further details). These devices are:

- Meta-Watch
- Non Invasive Blood Pressure (NIBP)
- Shimmer3 sensors

All devices communicate with the Virtual Task Execution through a Bluetooth connection.

With respect to the security requirements, data confidentiality is considered to be the most important issues in BAN. This implies to protect the patient data from disclosure by not leaking vital information to external or neighbouring networks.

There are several solutions to guarantee a suitable level of security in BAN, for instance the usage of public-key cryptography, although too costly, or the integration in the system of an external dedicated hardware for encryption and decryption of the data sent from each network's device (i.e. http://armor.tesyd.teimes.gr/).

In order to assess security in the BAN network of CogWatch system, the Secure Simple Pairing (SSP), embedded in the Bluetooth protocol [14], has been used to address security and simplicity of the pairing process.

The main aim of SSP is to maximize the security while minimizing the complexity of the end user. The method is based on a 6-digit numeric code, assigned for each device. The user must compare the numbers to ensure they are the same on each device. If the comparison succeeds, the devices are paired.

During pairing, an initialization key or master key is generated, using the E22 algorithm. The E0 stream cipher is used for encrypting packets, granting confidentiality, and is based on a shared cryptographic secret, namely a previously generated link key or master key. Those keys, used for subsequent encryption of data sent via the air interface, rely on the Bluetooth PIN, which has been entered into one or both devices.

This method provides an acceptable level of security, avoiding "man in the middle" (MITM) protection, assuming the user confirms on both devices and actually performs the comparison properly. Moreover, once a link key has been generated, an authenticated Asynchronous Connection-Less (ACL) link between the device and the VTE is encrypted in order to protect the data to be exchanged from eavesdropping.

Once pairing has been completed, a bond is created between each device and the VTE, enabling the devices to be automatically connected in the future without requiring to pairing process again. When desired, the user can later remove the bounding relationship.

In general, with respect to the type of data and level of privacy requested within the BAN network, the Bluetooth pairing guarantee an adequate level of security. In case an external source should try to access the data, the encryption key could protect the network for approximately 23.3 hours with the system running continuously. In order to ensure a high and safety level of protection, it is recommended to update the pairing code between the VTE and the device every at least one time a month.

Personal Area Network (PAN): The PAN network is a computer network used for transmits the data among different devices over cable or wireless network technologies, such as Bluetooth, ZigBee, etc.

The PAN network includes the modules belonging to the Patient Sub-System. The communication within this network is referring to the data transmitted between the VTE with BAN network devices and other monitoring and feedback devices belonging to the PAN network. Such devices include:

- Microsoft Kinect
- Leap Motion
- Coasters
- Microphone
- Toothpaste dispenser

With respect to the coasters, the communication between these sensors and the VTE are managed through pairing communication, described beforehand. The rest of the devices are directly connected to the VTE via USB.

Local Area Network (LAN): The LAN network includes the communication among Patient Sub-System to both the Professional Sub-System and to the Server Sub-System, as vice-versa.

With respect to the communication between Patient and Professional Sub-Systems, VTE and the CPI modules are involved. The link that allows the streaming data, exchanged between the two devices during the rehabilitation sessions, is based on local wire or wireless data connection.

Security requirements related to this connection include white listing and encryption/decryption protocols, described as follow:

- **White Listing**: In general, a whitelist access policy is a list of the users that are being provided a particular privilege, service, mobility, access or recognition. Those on the list will be accepted, approved or recognized. In a network policy access it represent a security model that controls access to external network resources. Thanks to the usage of the user identification, based on the IP-addresses registered on the whitelist, it is possible to limit the access of the patient and professional interfaces to only a dedicated number of users.
- **Data encryption/decryption**: Network encryption is a network security process that applies crypto services at the network transfer layer - above the data link level, but below the application level. The network transfer layers are layers 3 and 4 of the Open Systems Interconnection (OSI) reference model, the layers responsible for connectivity and routing between two end points. Using the existing network services and application software, network encryption is invisible to the end user and operates independently of any other encryption processes used. Data is encrypted only while in transit, existing as plaintext on the originating and receiving hosts. Network encryption is implemented through Internet Protocol Security (IPSec), a set of open Internet Engineering Task Force (IETF) standards that, used in conjunction, create a framework for private communication over IP networks. IPSec works through the network architecture, which means that end users and applications don't need to be altered in any way. Encrypted packets appear to be identical to unencrypted packets and are easily routed through any IP network.

Wide Area Network (WAN): A wide area network (WAN) is a network that exists over a large-scale geographical area. A WAN connects different smaller networks, including local area networks (LAN) and personal area networks (PAN). In the CogWatch system the WAN network include the entire system communication. The device connections involved in the WAN network are related to the communication between the CogWatch Server Sub-system and the CogWatch Web Portal, both being part of the Server Sub-System, and the communication between the CogWatch Server Sub-system and the Configuration module of the Patient Sub-System.

The security requirements related to both these connections are:

- **HyperText Transfer Protocol over Secure Socket Layer (HTTPS)**: The security of HTTPS is therefore that of the underlying TLS, which uses long-term public and secret keys to exchange a short-term session key to encrypt the data flow between

client and server. HTTPS provides authentication of the website and associated web server that one is communicating with, which protects against man-in-the-middle attacks. Additionally, it provides bidirectional encryption of communications between a client and server, which protects against eavesdropping and tampering with and/or forging the contents of the communication.[https://www.eff.org/https-everywhere/faq "HTTPS Everywhere FAQ". Retrieved 3 May 2012.] In practice, this provides a reasonable guarantee that one is communicating with precisely the website that one intended to communicate with (as opposed to an imposter), as well as ensuring that the contents of communications between the user and site cannot be read or forged by any third party.

- **User Authentication**: the most common method for authenticating a user's identity is to use a secret passphrase or password. Securing your network environment requires that strong passwords be used by all users. This helps avoid the threat of a malicious user guessing a weak password, whether through manual methods or by using tools, to acquire the credentials of a compromised user account.
- **White listing**: in order to prevent unauthorized users from using the system, a white list will be adopted, as for the LAN network security access. Only the users on a specific list will be accepted and approved to use the system.
- **Data encryption/decryption**: as described beforehand for the LAN network security, a network encryption, invisible to the user, will be integrated in the data communication.

  Encryption data is based on the generation of a persistent symmetric key using the Rijndael algorithm and then use this key to encrypt and decrypt a text string. The Rijndael algorithm represents the base of the Advanced Encryption Standard, a National Institute of Standards and Technology specification for the encryption of electronic data. The Rijndael algorithm [10] is a new generation symmetric block cipher, supporting key sizes of 128, 192 and 256 bits.
- **Firewall**: the patient profile and recording data, coming from the Configuration Module, are stored in the VTE repository. This information is sent and stored the central database in to the CogWatch HealthCare Subsystem. This operation is managed by a Web Services Description Language (WSDL). The WSDL is an XML-based interface. It provides an XML format to be transferred, managed and stored among different data sources.

  The CogWatch HealthCare Subsystem, in addition to the security protocols HTTPS for communication with the VTE, needs to be protected from potential unauthorized external access. A feasible and effective solution in the wide area networks is the use of a software firewall. A firewall is a product that serves to protect a computer or computers network from outside network attacks. Nowadays Internet attacks are increasing day by day. The most known attacks are the DoS or DDoS (Denial of Service or Distributed Denial of Service), which can cause damage also very annoying.

  The firewall analyses the traffic directed to a computer and blocks all data that can be harmful to the stability of the system. Not using a firewall would mean being exposed to thousands of potential attacks, without considering the possible unwanted visits to the system by hackers, crackers.

Firewalls use one or a combination of the following three methods to control traffic flowing in and out of the network:

Packet filtering: It is the most basic form of firewall software. It uses pre-determined security rules to create filters. When an incoming packet of information (small chunk of data) is flagged by the filters, it is not allowed through. Packets that make it through the filters are sent to the requesting system and all others are discarded.

Proxy service: A firewall proxy server is an application that acts as an intermediary between systems. Information from the internet is retrieved by the firewall and then sent to the requesting system and vice versa.

Stateful inspection: A 'stateful' firewall holds significant attributes of each connection in a database of trusted information, for the duration of the session. These attributes, which are collectively known as the 'state' of the connection, may include such details as the IP addresses and ports involved in the connection and the sequence numbers of the packets being transferred. The firewall compares information being transferred to the copy relevant to that transfer held in the database – if the comparison yields a positive match the information is allowed through, otherwise it is denied.

5.4.2 User authentication

The access to the clinician interface will be provided with an authentication login. Authentication is the method used to identify a user, machine or application and verifying this identity.

- Authentication will be done through the usernames and passwords. A cross-check data between username and password is implemented (LOG-IN module).
- The constraints about the definition of the password are at least 8 characters. In addition at least an uppercase letter must be present in the password.
- The limit for the number of unsuccessful trials of connection is three, after that the user is disabled and cannot access the web portal anymore. The technical team will receive a notification and will generate a new password for the clinician only after an explicit request of the user.
- All the connection attempts are logged on the system.

5.4.3 User Permission and roles

With respect to the user permission and roles, a set of access rights has been defined for accessing COGWATCH system. Depending on the user, a set of permissions allows to access to specific information and function of the system.

When a new user is created, a specific profile is associated with. Examples of access rights are inserting, deleting, updating, and viewing data.

Four different users' profiles are defined:

- Administrator: is in charge of maintaining and operating the Cogwatch system and network. The Administrator is not allowed to view patients' personal data as the

related sessions' rehabilitation data. In the P1.1 the main administrator's role is to create and monitor the users' accounts and verify user's identity.

- Clinician: is the healthcare provider working in a clinic or in the hospital. Usually is identified as the medical doctor that takes in care one or more patients.
- Therapist: is the person in charge of the rehabilitation session with AADS patients.
- Caregiver: is defined as patients' relative or friend, helping him with during the daily living activities.

The user roles are defined and assigned through the Account Manager module. The permission is assigned before the user authentication trough the Log-in module. For the table describing the roles and the specific permission of the users please consult the paragraph "5.2.1.2 User Permission and roles" of deliverable "D2.3.1 Report on networks I".

5.4.4 Software Tool for Data Security and Secure Communication Deployment

As already mentioned, the use of a vast range of tools for the exchange of sensitive information among different networks, must be taken into account within the problem of security. This is possible through the implementation of a set of tools and libraries, aimed at manage this complex and diversified architecture, all integrated in a security framework.

These security tools are deployed using the Microsoft .NET Framework [5]. For each type of communication and corresponding security issues, a specific set of .NET classes have been applied, as described in the following sections.

BAN Communication/Security: The communication is basing on the Bluetooth pairing connection, as described beforehand. Bluetooth connection is designed to run over a short-range wireless peer-to-peer network. As explained, if one or more devices are used as gateways to other networks, and if the security of Bluetooth is compromised, it could expose the device or its attached networks. The security model of Bluetooth is based on and enforced by two measures:

- Authentication
- Link encryption

There are different security modes to ensure security in Bluetooth connections [11]. The most appropriate one is to enforce the link encryption at the LMP (Link Management Protocol). Microsoft® Windows® CE .NET implements support for this mode security.

It is recommended to use a long passkey in order to prevent the correct link key from being easily computed. It is also important to not perform the pairing in a public places, to prevent an attacker from eavesdropping during the pairing phase.

Finally, the headset implementation must ensure each passkey's change is only possible over an authenticated and encrypted connection or Bluetooth link.

Software Tools for communication and security: the "Visual Studio .NET wireless communication library" is a powerful SDK for Bluetooth communication development. This library includes a complete components set for develop an application which should use

Bluetooth communication. It includes full components and classes set (Bluetooth Framework) that allows to enumerate and to manage local Bluetooth devices.

PAN Communication/Security: This network is designed for inexpensively connect low-power devices, located within few meters of the CogWatch VTE. The communication is based on Bluetooth. The security associated on this network is basing on the white listing and data encryption and decryption.

Software Tools for Development of PAN communication and security:

As for the BAN network, communication between PAN modules is managed by the "Visual Studio .NET wireless communication library".

LAN Communication/Security: The communication of the modules of the LAN network, as commented earlier, is based on white listing and data encryption and decryption.

Software Tools for Development of PAN communication and security:

White listing: A dynamic IP Restrictions Extension for Internet Information Services (IIS) will be used to ensure the IP addresses control. The dynamic IP Restrictions allows establishing a list of the IP addresses that have the rights to access to the application, while reducing the probabilities of the web application to be subject to an external attack.

Encryption/Decryption:

A .NET Security Framework will provide the implementation of different cryptographic algorithms based on ISO Security Architecture [22].

The.NET Framework, whose namespace is called System.Net, is based on Secure Sockets Layer (SSL), already integrated in the HTTPS communication. This security protocol allows sensitive information such login credentials to be transmitted securely.

WAN Communication: The communication is basing on https, user authentication, white listing and data encryption and decryption, already described.

Moreover, a firewall security access is present on CogWatch HealthCare Subsystem. A Windows firewall, a software component of Microsoft Windows, will provide firewalling and packet filtering functions. The firewall is controlled and configured through a COM object-oriented API. The firewall inspects and filters all IP version 4 (IPv4) and IP version 6 (IPv6) network traffic.

The firewall tracks the state of each network connection and determines whether the unsolicited incoming traffic should be allowed or dropped. Finally, it blocks the incoming traffic unless the traffic is a response to a request by the host or it is specifically allowed.

HTTPS and User authentication are described as following:

HTTPS: Communication is based on HTTPS, a communications protocol for secure communication over computer networks. It is based on layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol. SSL and TLS are cryptographic protocols designed to provide communication security over the Internet. By using HTTPS communication may prevent wiretapping and man-in-the-middle attacks.

User Authentication: The HTTPs supports the use of several authentication mechanisms to control access to pages and other resources. The authentication is the process of obtaining identification credentials, such as the user's name and password and validating those

credentials. Once the user has been authenticated, the authorization process determines whether that identity has access to a given resource.

Microsoft .NET implements authentication through authentication providers, the code modules that contain the code necessary to authenticate the requestor's credentials.

XML ENCRYPTION:

XML Encryption provides end-to-end security for applications that require a secure exchange of data. XML represents the most used technology for data, so the XML-based encryption is the natural way to handle complex requirements for security in data interchange applications. The XML encryption provides a mechanism for security requirements that are not covered by SSL, in particular the possibility to encrypt part of the data being exchanged and the secure sessions between more than two parties.

The data sent and received by the CogWatch HealthCare Subsystem are based on XML files. The encryption method uses an AES (Advanced Encryption Standard) session key to encrypt the XML files and then uses a public key to encrypt the AES session key.

In particular, the XML encryption has been used to encrypt the following information:

- From CogWatch HealthCare Subsystem to VTE Configuration module:
  - Schedule of new rehabilitation session. The data are related to the patient, timestamp and rehabilitation task information.
- From VTE Configuration module to CogWatch HealthCare Subsystem:
  - Rehabilitation session results, based on the patient, timestamp, video of the session and session information.

5.5 Privacy and confidentiality

As for CogWatch prototype P1.1, patients' data, stored locally in the VTE database, will be anonymized in P2. In the database no element will allow the possibility of identification of a subject. Internal algorithms are implemented to cross the data and present it to professionals. In this case, only statistic data (age and gender) will be available for the scientific community and patient identity will not appear in the rehabilitation session results. Patients will be identified by only an ID identifier.

Server, database backups and data recovery: Every user session is recorded in standard log files on the local database and sent to the server. According to the 2008 ASHRAE Environmental Guidelines for Datacom Equipment [24] the ambient temperature of server room must be hold between 20°C and 25°C. The equipment runs safely and efficiently. Data centres feature fire protection systems, including passive and active design elements, as well as implementation of fire prevention programs in operations. Smoke detectors are installed to provide early warning of a developing fire by detecting particles generated by smouldering components prior to the development of flame. Physical security also plays a large role with data centres. Physical access to the site is restricted to selected personnel, with controls including bollards and mantraps. Video camera surveillance is always present. Redundancy of the Internet connection is provided by using two upstream service providers (glass fibre and Digital Subscriber Line (DSL)). Network security elements are firewalls, Virtual private network (VPN) gateways, intrusion detection system. There is a monitoring system for the network and some of the applications. Power supply is made uninterruptible

by use of accumulators and voltage conversion. Backup: The Service is realized by a backup device to external media.

To resume, the security protocols adopted within the platform allow ensuring a high level of data security, in accordance with the Article 27 of the European Data Protection Directive (95/46/EC) [25].

The data protection and security requirements are also in line with the Data Protection Act [26] and both the .ICO anonymisation code of practice [27] and the HSCIC guide to confidentiality in health and social care [28].

Data recovery is enabled by back-service, separation between raw data files and database and mirroring of most sensitive data to the database “warehouse” storing a snapshot of the “upload & pre-process”-database and “Patient Record”-database.

6. CONCLUSIONS

CogWatch system aims at develop an AADS rehabilitation system based on highly instrumented objects and tools that are parts of the everyday environment of the patients. Using ad hoc algorithms, the sensorized objects can be used to monitor the behaviour and the progress of the rehabilitation therapy, as well as help AADS patients giving them real time feedback to carry out activities of daily living in an efficient way.

This deliverable is focused on the description of the general architecture of the second starting from the software development described in *"D2.3.1 Report on networks I"*. The improvement of the algorithms and protocols are defined starting from the deliverable *"D2.1 Report on system specification"* whose objectives were the analysis of system specifications and the definition of the architecture, and the conclusions obtained from the evaluation of the first Cogwatch prototype reported in *"D4.1.1 Report on technical evaluation I"* and *"D4.2.1 Report on Healthcare Evaluation I"*.

CogWatch system is composed by three main subsystems, the *Client Subsystem*, corresponding to the patient side used to perform rehabilitation sessions, the *CogWatch Professional Interface*, used by the professionals involved in the rehabilitation process to m monitor in real time the rehabilitation session remotely; and the Server Subsystem, in charge of supervising patient performance and progress in rehabilitation. This deliverable, describes in details the software modules and the communication procedure adopted in each subsystem. The updated version of the general architecture for the second prototype is reported in Section 2.

Section 3 describes the updated architecture and the software modules of the CogWatch Client Subsystem with a particular attention to the algorithms developed for the second prototype.

Section 4 is dedicated to the description of the CogWatch Professional Interface. A console application that allows the real-time remote monitoring of the rehabilitation session by the professionals involved in the rehabilitation process. At the same time, this application is useful to evaluate the reliability of the sensors and the AR algorithms.

Section 5 describes architecture of the CogWatch Server sub-system. There are no important changes with respect to the previous report, so the work has been referenced.

The last section describes in detail the security communication technologies aspects applied to the CW system.

The described architectures, technologies, protocols and software modules are based on the second version of the prototype of the system. Considering the continuous evaluation methodology adopted in the CW development, it is possible that the modules and algorithms described in this report will be improved based on the evaluation experiences. A full report of the finalised functionalities of the second prototype of the system will be detailed in *D4.1.2 Report on technical evaluation II"*.

REFERENCES

1. Andrew W. Williams, Soila M. Pertet, and Priya Narasimhan. “Tiresias: Black-Box Failure Prediction in Distributed Systems”. In: IPDPSIEEE (2007) , p. 1-8.
2. Bluetooth technology [online]. Available: http://www.bluetooth.com. Last Access: 12-November-2012].
3. Bowen A, West C, Hesketh A, Vail A. (2009). Rehabilitation for apraxia: evidence for short-term improvements in activities of daily living. Stroke, 40, 396-397.
4. Cesta, A., Cortellessa, G., Giuliani, M. V., Pecora, F., Scopelliti, M., & Tiberio, L. (2007). Psychological implications of domestic assistive technology for the elderly. PsychNology Journal, 5(3), 229–252.
5. Cryptographic Services in c# [online]. Available: http://msdn.microsoft.com/en-us/library/92f9ye3s.aspx [Last Access: 12-November-2012].
6. Errin W. Fulp, Glenn A. Fink, Jereme N. Haack. “Predicting Computer System Failures Using Support Vector Machines”. Proceedings of The First USENIX conference On Analysis Of System Logs. p.5-5, December 07, 2008, San Diego, California.
7. Felix Salfner. Predicting Failures with Hidden Markov Models, 2002.
8. Gary M. Weiss. “Timeweaver: a Genetic Algorithm for Identifying Predictive Patterns in Sequences of Events”. In proceedings of the Genetic and Evolutionary Computation Conference, 718-725 Morgan Kaufmann, San Francisco, CA, 1999.
9. Goldenberg G, Hangmann S. (1998). "Therapy of activities of daily living in patients with apraxia". Neuropsychological Rehabilitation. Vol. 8, 123-141.
10. Jamil, T. The Rijndael algorithm. Potentials, IEEE, DOI:10.1109/MP.2004.1289996, 2004.
11. Juha T. Vainio (25 May 2000). "Bluetooth Security". Helsinki University of Technology. Retrieved 1 January 2009
12. Levin, E., Pieraccini, R., Eckert, W., (2000), “A stochastic model of human-machine interaction for learning dialogue strategies”, *IEEE Transactions on Speech and Audio Processing*, Vol. 8, No. 1, January 2000, pp 11-23.
13. Li, Q. Observer-Based Fault Detection for Nuclear Reactor. Massachusetts Institute of Technology, 2001.
14. Lu, Yi; Serge Vaudenay. "Faster Correlation Attack on Bluetooth Keystream Generator E0". Crypto 2004: 407–425
15. Meingast M., Roosta T., Sastry S. Security and Privacy Issues with Healthcare Information Technology. Proceedings of the 28th IEEE EMBS Annual International Conference; New York, NY, USA. 31 August–3 September 2006; pp. 5453–5458
16. Nicholas Roach, “The effect of multimodal data sources in parallel on the accuracy and reliability of optical motion capture of human subjects”, PhD thesis, University of Birmingham, Birmingham, UK, 2011.
17. P . Tresadern, S. Thies, L. O. Kenney, D. Howard, and J. Y. Goulermas (2006). “Artificial neural network prediction using accelerometers to control upper limb FES

during reaching and grasping following stroke," in Proc. 28th Annu.Int. Conf. IEEE Engineering in Medicine and Biology Society. 2916-2919.

18. Parekh, M. and Baber, C., 2010, Tool use as gesture: new challenges for maintenance and rehabilitation, British Computer Society Human-Computer Interaction, http://ewic.bcs.org/upload/pdf/ewic_hci10_paper27.pdf
19. S. Young, G Evermann, M J F Gales, T. Hain, D. Kershaw, G.Moore, J. Odell, D. Ollason, D. Povey, V. Valtchev and P. Woodland, "The HTK book, version 3.4" , Cambridge University Engineering Department, 2006.
20. Salfner.F, M. Schieschke, and M.Malek. "Predicting Failures Of Computer Systems: A Case Study For A Telecommunication System". In Proceedings of IEEE International Parallel And Distributed Processing Symposium (Ipdps 2006), Dpdns Workshop, Rhodes Island, Greece, Apr. 2006.
21. Smania N, Girardi F, Domenicali C, Lora E, Aglioti S (2000) The rehabilitation of limb apraxia: a study in left-brain-damaged patients. Arch Phys Med Rehabil 81:379 –388.
22. System.Security.Cryptography Namespace. [online]. Available: http://msdn.microsoft.com/en-us/library/system.security.cryptography.aspx [Last Access: 12-November-2012].
23. Xiao Y., Shen X., Sun B., Cai L. Security and Privacy in RFID and Applications in Telemedicine. IEEE Commun. Mag. 2006;44:64–72
24. ASHRAE, T. 9.9, 2008. ASHRAE Environmental Guidelines for Datacom Equipment.
25. Cate, F. H. (1994). EU Data Protection Directive, Information Privacy, and the Public Interest, The. Iowa L. Rev., 80, 431.
26. Redsell, S. A., & Cheater, F. M. (2001). The Data Protection Act (1998): implications for health researchers. Journal of Advanced Nursing, 35(4), 508-513.
27. Information Commissioner Office (2012). Anonymisation: Managing Data Protection Risk Code of Practice.
28. Square, T., & Lane, B. (2013). A Guide to Confidentiality in Health and Social Care.