ALIoT

Internet of Things for Industry and Human Applications

Internet of Things for Healthcare Systems

TRAININGS

Funded by the Erasmus+ Programme of the European Union

Internet of Things for Industry and Human Applications

Internet of Things for Healthcare Systems

Newcastle University

LEEDS BECKETT UNIVERSITY

KTH VETENSKAP OCH KONST

UNIVERSIDADE D COIMBRA

ISTI

ЧНУ

1920

ХАІ

ТНЕУ

ЧДУ

НТУ

Vivere est cogitare

ІПМЕ НАН України

IT Альянс

SmartMe UNIVERSITY

Ministry of Education and Science of Ukraine
National Aerospace University "Kharkiv Aviation Institute"
Volodymyr Dahl East Ukrainian National University

V.S. Kharchenko, I.S. Skarga-Bandurova, T.O. Biloborodova, D.D. Uzun, A.A. Strielkina, O.O. Illiashenko, A.Y. Velykzhanin, O.V. Berezhnyi

Internet of Things for Industry and Human Applications

Internet of Things for Healthcare systems

Trainings

Edited by V.S. Kharchenko, I.S. Skarga-Bandurova

Project
ERASMUS+ ALIOT "Internet of Things: Emerging Curriculum for Industry and Human Applications"
(573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP)

2019

UDC 004.415/.416::61](076.5)=111

I-73

Reviewers: Dr. Ah-Lian Kor, Leeds Beckett University, Leeds, UK
DrS, Prof. Volodymyr Mokhor, director of Pukhov Institute for Modelling in Energy Engineering, corresponding member of NAS of Ukraine

I-73 V.S. Kharchenko, I.S. Skarga-Bandurova, T.O. Biloborodova, D.D. Uzun, A.A. Strielkina, O.O. Illiashenko, A.Y. Velykzhanin, O.V. Berezhnyi. **Internet of Things for Healthcare Systems**: **Trainings** / V.S. Kharchenko, I.S. Skarga-Bandurova (Eds.) – Ministry of Education and Science of Ukraine, National Aerospace University “KhAI”, Volodymyr Dahl East Ukrainian National University, 2019. – 93 p.

ISBN 978-617-7361-84-7
The materials of the training part of the study course ITM4 “IoT for Healthcare Systems”, developed in the framework of the ERASMUS+ ALIOT project “Internet of Things: Emerging Curriculum for Industry and Human Applications” (573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP).

The structure of work on verification of residual knowledge in the discipline, the corresponding training material, examples of tasks and criteria of evaluation are given. In the learning process, the theoretical aspects of IoT for healthcare systems are presented. The structures, models and technologies for development of healthcare IoT-based systems, advanced techniques and means for design, modernization and implementation of healthcare IoT-based systems and development and hardware optimization of units for IoT devices in healthcare systems are examined.

It is intended for engineers, developers and scientists engaged in the IoT for healthcare systems, for postgraduate students of universities studying in area of healthcare IoT-based systems, as well as for lecturers of relevant courses.

Ref. – 37 items, figures – 24, tables – 5, formulas – 11.

Approved by Academic Council of National Aerospace University “Kharkiv Aviation Institute” (record No 4, December 19, 2018).

ISBN 978-617-7361-84-7

Міністерство освіти і науки України
Національний аерокосмічний університет
ім. М. Є. Жуковського «Харківський Авіаційний Інститут”
Східноукраїнський національний університет ім. Володимира Даля

Харченко В.С., Скарга-Бандурова І.С., Білобородова Т.О., Узун Д.Д.,
Стрєлкіна А.А., Ілляшенко О.О., Великжанін А.Ю, Бережний О.В.

Інтернет речей для
індустріальних і гуманітарних застосунків

Інтернет речей для медичних систем

Тренінги

Редактори Харченко В.С., Скарга-Бандурова І.С.

Проект ERASMUS+ ALIOT
“Інтернет речей: нова освітня програма для потреб промисловості та суспільства”
(573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP)

2019

УДК 004.415/.416::61](076.5)=111
І-73

Рецензенти: Др. А-Ліан Кор, Leeds Beckett University, Велика Британія

Д.т.н., проф. Володимир Мохор, директор інституту проблем моделювання в енергетиці ім. Г.Є. Пухова, член-кореспондент НАН України

В.С. Харченко, І.С. Скарга-Бандурова, Т.О. Білобородова, Д.Д. Узун, А.А. Стрєлкіна, О.О. Ілляшенко, А.Ю. Великжанін, О.В. Бережний.

І-73 **Інтернет речей для медичних систем. Тренінги** / За ред. В. С. Харченка, І. С. Скарги-Бандурової. - Міністерство освіти і науки України, Національний аерокосмічний університет «ХАІ», Східноукраїнський національний університет ім. Володимира Даля, 2019. - 93 с.

ISBN 978-617-7361-84-7

Викладено матеріали тренінгової частини курсу ITM4 “IoT для медичних систем”, підготовленого в рамках проекту ERASMUS+ ALIOT “Internet of Things: Emerging Curriculum for Industry and Human Applications” (573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP).

Наведена структура робіт з перевірки знань з курсу, відповідний тренінговий матеріал, приклади виконання завдань та критерії оцінювання. В процесі навчання наводяться теоретичні аспекти IoT для медичних систем. Вивчаються структури, моделі та технології розробки медичних IoT систем, сучасні методики і засоби проектування, модернізації та впровадження медичних IoT систем, а також розробка та апаратна оптимізація компонент IoT пристроїв в медичних системах.

Призначено для інженерів, розробників та науковців, які займаються розробкою та впровадженням IoT для медичних систем, для аспірантів університетів, які навчаються за напрямом IoT систем, а також для викладачів відповідних курсів.

Бібл. – 37, рисунків – 24, таблиць – 5, формул – 11.

Затверджено Вченою радою Національного аерокосмічного університету «Харківський авіаційний інститут» (запис № 4, грудень 19, 2018).

УДК 004.415/.416::61](076.5)=111

ISBN 978-617-7361-84-7

ABBREVIATIONS

ADC – Analog-to-digital converter

ARIMA – Autoregressive Integrated Moving Average

BE – Base Event

BIC – Bayesian Information Criterion

BPA – Base Probability Assignment

CBE – Coincident Base Events

CPU – Central Processing Unit

CSV – Comma-Separated Values

DCSM – Discrete-Continuous Stochastic Model

DHCP – Dynamic Host Configuration Protocol

ECG – Electrocardiogram

EEG – Electroencephalography

EMG – Electromyography

EP – End of Procedure

FCVTI – Formula for calculating the value of the transition intensity

FIPS – Federal Information Processing Standard

GPIO – General-Purpose Input/Output

HIMSS – Healthcare Information and Management Systems Society

HIPAA – Health Insurance Portability and Accountability Act

HITECH – Health Information Technology for Economic and Clinical Health Act

HL7 – Health Level 7

Hz – Hertz

ID – Identifier

IoHT – Internet of Healthcare Things

IoMT – Internet of Medical Things

IoT – Internet of Things

ISO – International Organization for Standardization

JSON – JavaScript Object Notation

NB-IoT – Narrow Band Internet of Things

NIST – National Institute of Standards and Technology

PACP – Probabilities of Alternative Continuation of the Process

PHI – Protected Health Information

RF – Radio Frequency

SAM – Structural Automaton Model

SDP – Specification of Developed Project

SSID – Service Set Identifier

WBAN – Wearable Body Area Network

INTRODUCTION

The materials of the training part of the study course ITM4 “IoT for healthcare systems”, developed in the framework of the ERASMUS+ ALIOT project “Internet of Things: Emerging Curriculum for Industry and Human Applications” (573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP)[1].

The structure of work on verification of residual knowledge in the discipline, the corresponding training material, examples of tasks and criteria of evaluation are given. In the learning process, the theoretical aspects of IoT for healthcare systems are presented. The structures, models and technologies for development of healthcare IoT-based systems, advanced techniques and means for design, modernization and implementation of healthcare IoT-based systems and development and hardware optimization of units for IoT devices in healthcare systems are examined.

Theoretical issues for “IoT for Industrial Systems” are described in Part XII (sections 44-47) of the book [*Internet of Things for Industry and Human Application*. In Volumes 1-3. Volume 3. Assessment and Implementation / V. S. Kharchenko (ed.) – Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019].

The module ITM4.1 “IoT Infrastructure for healthcare systems” includes one seminar one training. The seminar is exploring of existing and promising principles, methods, tools, technologies of the healthcare Internet of Things implementation. The training is aimed to develop a model of a functional behavior of a smart healthcare device in a form of a structural automaton model.

The module ITM4.2 “Security and privacy for healthcare systems” includes one seminar one training. The seminar is exploring of existing normative base for the privacy and security of the healthcare Internet of Things. The training is aimed to develop and investigate Markov models set for the healthcare IoT infrastructure that allows taking into account the specificity of end user devices, communication channels, technologies of data flows and safety and security issues of these components.

[1] *The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.*

The module ITM4.3 “Wearable and Embedded IoT-based solutions for biomedical applications” includes three trainings. The first training is an introduction to IoT wearable system for biomedical monitoring. The training study design, architecture and hardware of IoT wearable system for biomedical monitoring. The second training is the foundation to IoT network configuration for biomedical monitoring. The training study data channels, network hardware setting, data acquisition, and transmission technique. Configure wearable device, network hardware, and software for ECG monitoring data transmission to server and ECG signal visualization. The third training is study of approaches to biomedical monitoring data analysis. The training study biomedical data analysis for real-time monitoring using data fusion technique.

The module ITM4.4 “Devices with reconfigurable architecture for biomedical IoT based applications” includes 3 trainings. The first training is exploring the stage of smartphone application development for monitoring human vital signs using smartphone sensors data. The second training is configuration of smartphone IoT based application for sensor data transmission to cloud storage and dashboard for human vital signs monitoring. The third training is discovering of approaches to real-time data processing and analysis.

The course is intended for engineers, developers and scientists engaged in the IoT for healthcare systems, for postgraduate students of universities studying in area of healthcare IoT-based systems, as well as for lecturers of relevant courses.

The training was prepared by Professor, DrS. V.S. Kharchenko (National Aerospace University “KhAI”), Professor, DrS. I.S. Skarga-Bandurova, Dr. T.O. Biloborodova (Volodymyr Dahl East Ukrainian National University), Dr. D.D. Uzun, A.A. Strielkina, Dr. O.O. Illiashenko (National Aerospace University “KhAI”), A.Y. Velykzhanin, O.V. Berezhnyi (Volodymyr Dahl East Ukrainian National University). General editing was performed by Head of Computer Systems, Networks and Cybersecurity Department of National Aerospace University “KhAI”, Professor, DrS. V.S. Kharchenko.

The authors are grateful to the reviewers, project colleagues, staff of the departments of academic universities, industrial partners for valuable information, methodological assistance and constructive suggestions that were made during the course program discussion and assistance materials.

IOT INFRASTRUCTURE FOR HEALTHCARE SYSTEMS

V.S. Kharchenko, D.D. Uzun and A.A. Strielkina

Seminar 1
INTERNET OF HEALTHCARE THINGS: TRENDS, PROBLEMS AND SOLUTIONS

1. Seminar objectives

The objectives are to provide knowledge and practical skills on:

– preparation of a report (analytical review or vision and brief specification of developed project – SDP) on analysis of development and implementation of IoT in healthcare and medicine;

– preparation of a ppt presentation according with report results for short lecture/seminar for other students;

– presentation and defence of received results.

2. Seminar preparation

Seminar preparation includes the following steps.

1) Assignment (choice) of report subject (analytical review, SDP) and tasks specification.

The report subject is to be agreed with the lecturer. It can be chosen by students on their own based on the following suggested list:

– principles, methods, tools, technologies…;

– Internet of medical/healthcare things, IoHT/IoMT architectures, data transfer, Internet routing…;

– sensors, sensor devices, intelligent endpoints, energy sources, power control of IoHT/IoMT …;

– wireless personal area network, WPAN, 802.15 standards, Bluetooth, IEEE 802.15.4, Zigbee in IoHT/IoMT …;

– cloud computing, fog computing, edge computing in IoHT/IoMT…;

– cyber security, safety, physical security, privacy of IoHT/IoMT;

– AI, machine learning, neural nets in IoHT/IoMT… .

Suggested report subjects (can be extended):

– Internet of Things in healthcare: applications, benefits, and challenges;

– Internet of Things in healthcare in Ukraine and EU;

– Landscape based analysis of development and implementation of Internet of Things in healthcare;

– Analysis of Big Data implementation in IoHT/IoMT;

– Analysis of standards for IoHT/IoMT (ISO, IEC, IEEE, FDA, HIPAA and others);

– Cyber security and privacy issues in IoHT/IoMT;

– Signal processing from smart sensors technologies in IoHT/IoMT;

– Analysis of machine learning driven healthcare Internet of Things;

– Design and implementation technologies of healthcare Internet of Things infrastructure;

– Social Internet of Things in healthcare.

Report subject is to be agreed with the lecturer and consist with the subject area of the course (IoT and modern technologies for healthcare and medicine).

2) Work plan development and responsibility assignment among target group members. Work plan can be presented as a Gantt chart that includes the main events, time-frames and assignment of responsibility among the target group members.

The target group consists of 3 persons. Time resource is 9x3=27 hours (+20 minutes for the presentation and defence). The responsibility assignment is determined by the group members.

Suggested responsibility assignment:

– manager responsible for planning and coordination of activities and presents the idea on the seminar (1st part of the overall report - task statement),

– analyst or system developer (2nd part of the report),

– application developer (3rd part of the report and style concept).

3) Search of the information about report subject (library, the Internet, resources from department) and primary analysis. The search of the information is conducted using the keywords given in paragraph 2.1. Methodological guidelines and the selected readings are given individually (per groups). Please use reference list [1-10]. Theoretical issues for healthcare IoT are described in Part XII (sections 44-47) of the book [1].

4) Report and presentation plans development. Report plan includes:

– introduction (relevance, reality challenges, brief analysis of the problem – references, purpose and tasks of the report, structure and contents characteristics);

– systematized description of the main report parts (classification schemes, models, methods, tools, technologies, selection of indexes and criteria for assessment, comparative studies, correlation between standards and requirements);

– conclusions (established goal achievement, main theoretical and practical results, result validity, ways of further work on the problem);

– list of references;

– appendixes.

5) Report writing. The report should stand for 15-20 A4 pages (font size 14, spacing 1.5., margins 2 cm) including the title page, contents, main text, list of references, appendixes. Unstructured reports or reports compiled directly from Internet sources (more 50%), having incorrect terms and no conclusion shall not be considered.

The work plan and responsibility assignment (Gantt chart), presentation slides and an electronic version of all material related to the work are required to be included in appendixes.

6) Presentation preparation. The presentation is to be designed in PowerPoint and be consistent with the report plan (10-15 slides); the time-frame for the presentation is 15 minutes.

The presentation should include the slides as follows:

– title slide (specification of the educational institution, department, course of study, report subject, authors, date);

– contents (structure) of the report;

– relevance of the issues covered, the purpose and the tasks of the report based on the relevance analysis;

– slides with the details of the tasks;

– report conclusion;

– list of references;

– testing questions.

Each slide should include headers with the report subject and authors.

The contents of the slides should include the keywords, figures, formulas rather than the parts from the report.

The information can be presented dynamically.

3. Presentation and defence

The presentation should be given at the seminar for 20 minutes including:

– presentation (10-15 minutes);

– discussion (5-10 minutes).

Time schedule can be specified by lecturer.

4. Report assessment

The work is assessed on the following parameters:

a) report text quality (form and contents),

b) presentation quality (contents and style),

c) report quality (contents, logical composition, timing shared among parts, conclusion),

d) fullness and correctness of the answers.

Each student is given an individual mark for the report and the presentation based on the results and responsibility assignment.

5. Recommended literature

1. V. S. Kharchenko (ed.), “*Internet of Things for Industry and Human Application. In Volumes 1-3. Volume 3. Assessment and Implementation*”, Ministry of Education and Science of Ukraine, National Aerospace University “KhAI”, 740 p., 2019.

2. S. Islam, D. Kwak, M. Humaun Kabir, M. Hossain and K. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey", *IEEE Access*, vol. 3, pp. 678-708, 2015. Available: 10.1109/access.2015.2437951.

3. D. Krishnan, S. Gupta and T. Choudhury, "An IoT based Patient Health Monitoring System", *2018 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, 2018. Available: 10.1109/icacce.2018.8441708.

4. "IoT - Internet of Things | IoT Network Protocols", Lessons-tva.info, 2018. [Online] (in Russian). Available: www.lessonstva.info/articles/net/013.html.

5. A. Laya, “The Internet of Things in Health, Social Care, and Wellbeing”, Doctoral Thesis, KTH Royal Institute of Technology, 2017.

6. BI Intelligence. The global market for IoT healthcare tech will top $400 billion in 2022. [Online]. Available: www.businessinsider.com/the-global-market-for-iot-healthcare-tech-will-top-400-billion-in-2022-2016-5.

7. J. Healey, N. Pollard, B. Woods. The healthcare Internet of things: rewards and risks.

8. A. Mohan. Cyber Security for Personal Medical Devices Internet of Things. *Proceedings of the IEEE International Conference on Distributed Computing in Sensor Systems*, 26-28 May, 2014, pp. 372-374.

9. S. Baker, W. Xiang and I. Atkinson, "Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities", *IEEE Access*, vol. 5, pp. 26521-26544, 2017.

10. P.A. Laplante, M. Kassab, N.L. Laplante, J.M. Voas, J. “Building Caring Healthcare Systems in the Internet of Things,” *IEEE Systems Journal*, pp. 1-8, 2017.

Training 1
FUNCTIONAL BEHAVIOR OF NETWORKED HEALTHCARE DEVICE MODELING

1. Objectives and tasks

Goal and objectives: This training is exploring the stage of the networked healthcare devices modeling.

Learning objectives:

− study the functional characteristics abilities of the networked healthcare devices to be modelled;

− study of discrete-continuous stochastic modeling abilities for healthcare IoT infrastructure research.

Practical tasks:

− acquire practical skills in development of discrete-continuous stochastic models;

− acquire practical skills in modeling of the networked healthcare devices;

− get skills to formulate recommendations and make decisions concerning choice of hardware and software components and architecture for IoT healthcare system considering requirements to reliability, security and availability.

Exploring tasks:

− investigate the process of discrete-continuous stochastic models' development;

− analyze dependencies of successful implementation of all tasks and time for different indicators.

Setting up

In preparation for training it is necessary:

− to clear the goals and mission of the research;

− to study theoretical material contained in this manual, and in [1-3];

− to familiarize oneself with the main procedures and specify the exploration program according to the defined task.

Recommended software:

− ASNA software [3].

Synopsis

In this training, you will learn a process of a discrete-continuous stochastic model (DCSM) of a functional behavior of a smart healthcare device in a form of a structural automaton model (SAM) development.

2. Brief theoretical information

The task of modeling the functional behavior of healthcare IoT systems is in demand and relevant. It is proposed to develop a discrete-continuous stochastic model of the functional behavior of the networked healthcare device in a form of the structural automaton model. The object of research is the healthcare device that operates in the IoT environment. The indicator of the healthcare device using effectiveness is a probability a successful execution of the task for the determined time.

A list of procedures will serve as the basis for determining the basic events necessary for the development of the SAM. During developing of the model of functional behavior of the healthcare device, its composition and separate components should be described using the corresponding indicators and parameters of functionality. In fact, performing of each procedure in the fault-tolerant systems (in this case, in healthcare systems) is not absolutely successful, the probability of the successful completion of any procedure is $P<1$.

Development of the discrete-continuous stochastic model (DCSM) is performed in accordance with the methodologies described in [2]. This methodology involves: determining the basic events of the functional behavior of the research object; compiling a list of indicators and parameters of functionality, which should be taken into account in the DCSM; forming a state vector (assigning a component to the state vector in accordance with the requirements for the adequacy degree of the model); developing a reference graph of states; developing of a structural automaton model (SAM), including its verification; validation of DCSM.

During the SAM development it is necessary to take into account all the procedures and processes that occur during the operation of the healthcare device. Procedures are characterized by events beginning (BP), ending and average duration values. End-of-procedure (EP) events are accepted for basic events (BE). Non-compliance events, as well as procedures with an average duration value of 0, are presented as coincident base events (CBE).

The ASNA software solves the linear homogeneous differential equations, which is presented in the form of probabilities of staying in the states.

3. Execution order

1. Choose a smart healthcare device to be modelled.
2. Conduct an analysis of its functional behavior in verbal form using technical specifications given by the device manufactures. Provide this description.
3. Outline main procedures that occur during device functioning. Fill in Table 2.1 with this list of procedures, their indicators (probability of successful procedure implementation; symbols) and parameters (an average time for the procedure duration in seconds, minutes or hours; should be taken from technical specifications given by the device manufactures).

Table 2.1 − Indicators and parameters of devices functioning procedures

№	Procedure	Indicator	Parameter	
		Symbol	Symbol	Value
1				
…				

4. Outline base events and coincident base events that are characterized as the end of certain procedure; give to each of them number in the form like BE1, …., BEN or CBEM.
5. Define components of the state vector in a verbal form or as Table 2.2.

Table 2.2 − Components of the state vector

Component of the state vector	Purpose	Value
V1	Current state of …	0 – ….; 1 – …..; N – ….
V2		
…		

6. Develop a develop of a reference graph. The initial data are basic events (BE), indicators and parameters of functionality in a form as presented in Table 2.3.

Table 2.3 − An example of a reference graph

№ step	Previous state under consideration and the current BE	PACP	States of the object			№ state	Transition from state to state	FCVTI
			V1	…	VN			
1	Initial state	--	0	…	0	1	--	--
2	1BE1	P	1	…	0	2	1 → 2	P*1/T
3	1BE1 (CBE2)	1 – P	2	…	0	3	1 → 3	(1-P)*1/T
…								

7. Use the software ASNA to investigate the developed model. Verify the developed model to be sure that it constructs the graph of states and transitions correctly.

8. Using software ASNA build dependencies of successful implementation of all tasks and time for different indicators (probability of the successful procedure implementation). Show the procedures that have the biggest influence on the indicator of the successful procedure implementation.

9. Document the research process.

10. Draw a conclusion.

4. Requirements to the content of the report

− title page;
− research purpose and program;
− description of the object of research;
− description of stages of model development;
− results of the modeling;
− conclusions.

5. Test questions

1. What are steps of the DCSM development?
2. For what reason the software ASNA is used?

3. What is the state vector?
4. By what each procedure is characterized?
5. What is the reference graph?

6. Recommended literature

1. V. S. Kharchenko (ed.), “*Internet of Things for Industry and Human Application. In Volumes 1-3. Volume 3. Assessment and Implementation*”, Ministry of Education and Science of Ukraine, National Aerospace University “KhAI”, 740 p., 2019.
2. D. Fedasyuk and S. Volochiy, "Method of developing the structural-automaton models of fault-tolerant systems", *2017 14th International Conference on The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM)*, 2017. Available: 10.1109/cadsm.2017.7916076.
3. B. Volochiy, B. Mandziy and M. Ozirkovskyi, "Extending the Features of Software for Reliability Analysis of Fault-tolerant Systems", *Computational problems of electrical engineering*, vol. 2, no. 2, pp. 113-121, 2012.

SECURITY AND PRIVACY FOR HEALTHCARE SYSTEMS

V.S. Kharchenko, D.D. Uzun, A.A. Strielkina, O.O. Illiashenko

Seminar 1
ANALYSIS OF NORMATIVE PROFILE-GENERATED BASE FOR SECURITY AND PRIVACY OF HEALTHCARE SYSTEMS

1. Seminar objectives

The objectives are to provide knowledge and practical skills on:

– preparation of a report (analytical review or vision and brief specification of developed project – SDP) on analysis of normative base for security and privacy of healthcare systems;

– preparation of a ppt presentation according with report results for short lecture/seminar for other students;

– presentation and defence of received results.

2. Seminar preparation

Seminar preparation includes the following steps.

1) Assignment (choice) of report subject (analytical review, SDP) and tasks specification.

It is needed to choose by students on their own a healthcare device to be analyzed. It is to be agreed with the lecturer.

Using giving by lecture software obtain a list of standards and requirements to cybersecurity and privacy of healthcare devices (Fig. 1.1).

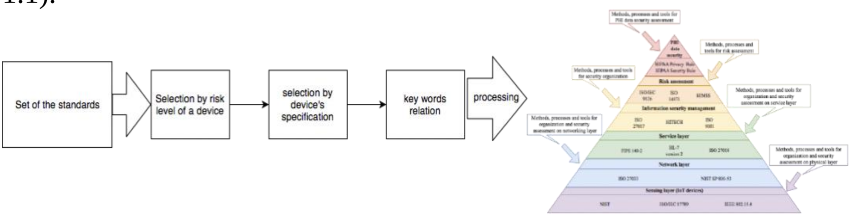

Fig. 1.1 – A process of getting the list of normative documents

It is needed to construct hierarchical model for healthcare IoT system for chosen research object (see Fig. 1.2 as example).

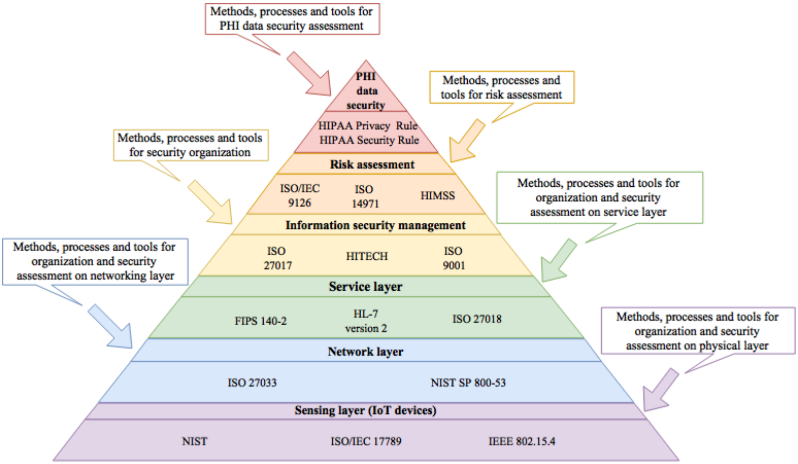

Fig. 1.2 – Hierarchical model for healthcare IoT system

At the lower (sensing) level of the developed model the standards for the end devices to be analyzed should be determined. Network security that includes devices, security of management activities associated with the devices, applications/services, and end-users, in addition to the information being transferred security – ISO 27033 and represents the security controls and associated assessment procedures – NIST 800-53. Service layer has to be protected by standards for clouds and service configurations such as FIPS 140-2 for static data, ISO 27018 for protecting data in a cloud and Health Level 7 for transfer medical data between software applications used by various providers. Normative documents which are presented there explains how to work with sensitive medical data (HIPAA), how to organize security in healthcare and medical systems (Health Information Technology for Economic and Clinical Health (HITECH), ISO 27017) and how to reduce risks associated with humans' life. Information security management layer gives guidance and recommendations guidance on the cloud security aspects (ISO 27017), improving healthcare quality, safety and efficiency, testing (HITECH) and a system of quality management (ISO 9001). Risk assessment layer has standards for the evaluation of quality (ISO/IEC 9126), risk management for medical devices (ISO 14971) and a compliance with Healthcare Information and Management Systems Society (HIMSS). PHI data security layer consists of the rules that institute policies and procedures for maintaining the privacy and the security of individually identifiable health information, outlines numerous attacks relating to healthcare, and establishes civil and criminal penalties.

Report is to be consist necessarily with the security and privacy requirements profile to the healthcare devices.

Report subject is to be agreed with the lecturer and consist with the subject area of the course (IoT and modern technologies for healthcare and medicine).

2) Work plan development and responsibility assignment among target group members. Work plan can be presented as a Gantt chart that includes the main events, time-frames and assignment of responsibility among the target group members.

The target group consists of 3 persons. Time resource is 9x3=27 hours (+20 minutes for the presentation and defence). The responsibility assignment is determined by the group members.

Suggested responsibility assignment:

– manager responsible for planning and coordination of activities and presents the idea on the seminar (1st part of the overall report - task statement),

– analyst or system developer (2nd part of the report),

– application developer (3rd part of the report and style concept).

3) Search of the information about report subject (library, the Internet, resources from department) and primary analysis. The search of the information is conducted using the keywords given in paragraph 2.1. Methodological guidelines and the selected readings are given individually (per groups). Please use reference list [1-3]. Theoretical issues for healthcare IoT are described in Part XII (sections 44-47) of the book [1].

4) Report and presentation plans development. Report plan includes:

– introduction (relevance, reality challenges, brief analysis of the problem – references, purpose and tasks of the report, structure and contents characteristics);

– systematized description of the main report parts (classification schemes, models, methods, tools, technologies, selection of indexes and criteria for assessment, comparative studies, correlation between standards and requirements);

– conclusions (established goal achievement, main theoretical and practical results, result validity, ways of further work on the problem);

– list of references;

– appendixes.

5) Report writing. The report should stand for 15-20 A4 pages (font size 14, spacing 1.5., margins 2 cm) including the title page, contents, main text, list of references, appendixes. Unstructured reports or reports compiled directly from Internet sources (more 50%), having incorrect terms and no conclusion shall not be considered.

The work plan and responsibility assignment (Gantt chart), presentation slides and an electronic version of all material related to the work are required to be included in appendixes.

6) Presentation preparation. The presentation is to be designed in PowerPoint and be consistent with the report plan (10-15 slides); the time-frame for the presentation is 15 minutes.

The presentation should include the slides as follows:

– title slide (specification of the educational institution, department, course of study, report subject, authors, date);

– contents (structure) of the report;

– relevance of the issues covered, the purpose and the tasks of the report based on the relevance analysis;

– slides with the details of the tasks;

– report conclusion;

– list of references;

– testing questions.

Each slide should include headers with the report subject and authors. The contents of the slides should include the keywords, figures, formulas rather than the parts from the report.

The information can be presented dynamically.

3. Presentation and defence

The presentation should be given at the seminar for 20 minutes including:

– presentation (10-15 minutes);

– discussion (5-10 minutes).

Time schedule can be specified by lecturer.

4. Report assessment

The work is assessed on the following parameters:

a) report text quality (form and contents),

b) presentation quality (contents and style),

c) report quality (contents, logical composition, timing shared among parts, conclusion),

d) fullness and correctness of the answers.

Each student is given an individual mark for the report and the presentation based on the results and responsibility assignment.

5. Recommended literature

1. V. S. Kharchenko (ed.), "*Internet of Things for Industry and Human Application. In Volumes 1-3. Volume 3. Assessment and Implementation*", Ministry of Education and Science of Ukraine, National Aerospace University "KhAI", 740 p., 2019.

2. A. Chacko, T. Hayajneh, "Security and Privacy Issues with IoT in Healthcare", EAI Endorsed Transactions on Pervasive Health and Technology, vol. 4, is. 14, 7 p., 2018.

3. A. Mohan. Cyber Security for Personal Medical Devices Internet of Things. Proceedings of the IEEE International Conference on Distributed Computing in Sensor Systems, 26-28 May, 2014, pp. 372-374.

Training 1
MODELING OF CYBER SECURITY PROCESSES OF IOT HEALTHCARE SYSTEMS

1. Objectives and tasks

Goal and objectives: This training is exploring the stage of the cyber security processes of IoT healthcare systems modeling.

Learning objectives:

− study the functional characteristics abilities of the healthcare IoT cybersecurity processes to be modelled;

− study of discrete-continuous stochastic modeling abilities for healthcare IoT infrastructure cybersecurity research.

Practical tasks:

− acquire practical skills in development of discrete-continuous stochastic models in a form of Markov models;

− acquire practical skills in modeling and simulating of the healthcare IoT cybersecurity processes;

− get skills to formulate recommendations and make decisions concerning choice of hardware and software components and architecture for IoT healthcare system considering requirements to reliability, security and availability.

Exploring tasks:

− investigate the process of discrete-continuous stochastic models' in a form of Markov models development;

− analyze dependencies to getting to the stationary state and different values of attacks intensities.

Setting up

In preparation for training it is necessary:

− to clear the goals and mission of the research;

− to study theoretical material contained in this manual, and in [1]-[4];

− to familiarize oneself with the main procedures and specify the exploration program according to the defined task.

Synopsis

In this training, you will learn a process of a discrete-continuous stochastic model abilities for healthcare IoT infrastructure cybersecurity development and simulation.

2. Brief theoretical information

There are several types of attacks on IoT that were discussed in many papers [2] – [4]. The main categories of IoT attacks are aimed for control, data, controllers (end-nodes) and networks. Attacks on data are very devastating in the healthcare field due to the physician–patient privilege and a patient privacy and confidentiality. Attacks on control involve imply an intruder's intention to gain access to the management of both the entire healthcare IoT system and individual components. Attacks on controllers are aimed at end-nodes (patients' devices) to gain access to control them and make a physical damage. Attacks on networks are aimed to sniffing out, copying the confidential information or any other data flowing in the networks.

After analysing classification of attacks according the main aims and focus is presented in Fig. 2.1.

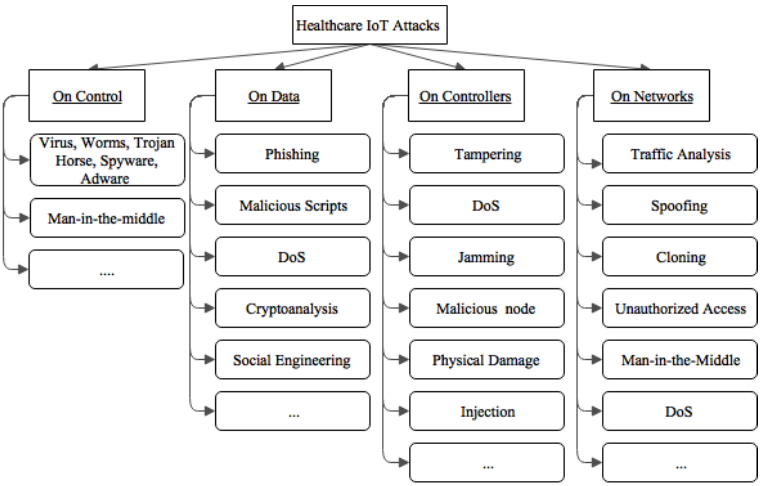

Fig. 2.1 – Classification of the healthcare IoT attacks

Such attacks on vulnerabilities can prevent the devices and infrastructure to communicate correctly and without failures.

In general, in the healthcare IoT system, the failures of single (or attacks on) subcomponents are possible. These failures may lead to the failures of the main components of infrastructure (i.e. medical device, cloud, etc.). In its turn, the failures of main components may lead to failure of the whole healthcare IoT system. Fig. 4.4 shows the dependence of the healthcare IoT system failures, where state 0 corresponds to condition when there is no any failure in the system, state 1 – there is one failure (of subcomponent), state 2 – there are two failures (subcomponent and main element), state 3 – there are three failures (the failure of the whole healthcare IoT system).

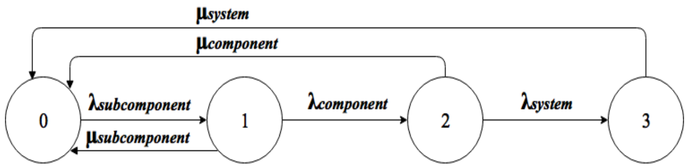

Fig. 2.2 – Dependence of the healthcare IoT failures.

Fig. 2.3 shows a Markov's graph of the main components functioning of the healthcare IoT system during attacks, λ - the failure and/or attack rate, μ - the recovery and/or reflection rate. Thereby, the basic states of the healthcare IoT system are: 1 - normal condition (upstate) system; 2 – traffic analysis attack; 3 – spoofing attack; 4 – cloning attack; 5 – unauthorized access to the network or database; 6 – failure of the network; 7 – failure due the data leakage; 8 – man-in-the-middle attack; 9 – DoS/DDoS attack; 10 – failure due the loss of control; 11 – attacks on software (i.e., viruses, worms, Trojan horses, spyware, adware, etc.); 12 – phishing attack; 13 – malicious scripts injection attacks; 14 – social engineering; 15 – failure or controllers (hardware, end-nodes); 16 – tampering of the end-nodes attack; 17 – jamming attack; 18 – malicious node injection attack; 19 – physical damage; 20 – complete failure of healthcare IoT system.

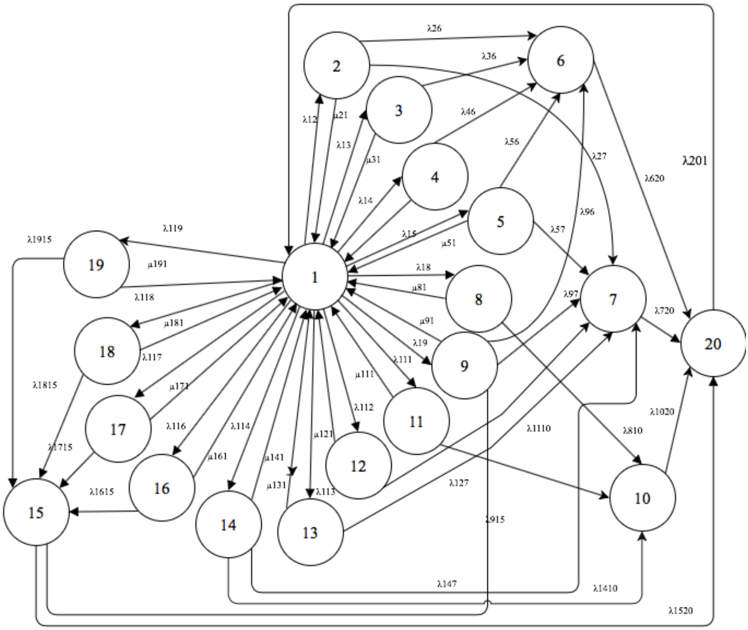

Fig. 2.3 – Markov's graph of attacks on the healthcare IoT infrastructure

Such Markov model for the healthcare IoT system can be divided into four levels: the first level is the upstate (state 1), the second level are the states state the transition to which occurred due to attacks (states 2-5, 8, 9, 11-14, 16-19), the third level implies states with different failures (states 6, 7, 10, 15); the fourth level is a failure of a whole system (state 20). So, there is only one up-state in the considering system.

3. Execution order

1. Find the statistics on attacks probabilities, intensities and/or use experts assessments for single unknown data.

2. Simulate the model for (a) one attack from each subcategory (Fig. 2.1), (b) one category (choose by students on their own) and (c*) all types of attacks, separately. The tool or programming language for simulation is chosen by students on their own.

The process of the model simulation may be as follows:

– entering the initial values (intensities, probabilities, average duration of attacks, etc.);

– constructing the transition matrix;

– simulation of the model using standard functions and obtaining of the steady states (e.g., for R language for the discrete continious markov models the function *steadyStates(object)* from library *Markovchain* may be used).

3. Build dependencies of (a) getting to the stationary state for 2.a, 2.b and 2.c (from previous paragraph); (b) getting to the stationary state for 2.b for different intensities of attacks. Give an analysis of the obtained results.

4. Document the research process.

5. Draw a conclusion.

4. Requirements to the content of the report

− title page;
− research purpose and program;
− description of the object of research;
− description of stages of model development;
− results of the modeling;
− conclusions.

5. Test questions

1. What types of attacks are the healthcare IoT infrastructure affected?

2. What are the consequences of a successful attack on the healthcare IoT infrastructure?

3. Describe interconnection between the healthcare IoT infrastructure failures.

4. Describe steps to simulate the developed Markov model.

6. Recommended literature

1. V. S. Kharchenko (ed.), “*Internet of Things for Industry and Human Application. In Volumes 1-3. Volume 3. Assessment and Implementation*”, Ministry of Education and Science of Ukraine, National Aerospace University “KhAI”, 740 p., 2019.

2. M. Abomhara, and G. M. Kien, “Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks,” *J. Cyber*

Secur. Mobil, vol. 4, no. 1, 2014, pp. 65-88. DOI: 10.13052/jcsm2245-1439.414.

3. M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, “A Critical Analysis on the Security Concerns of Internet of Things (loT)”, in *International Journal of Computer Applications*, vol. 111, 2015, 6 p. DOI: 10.5120/19547-1280.

4. M. Nawir et al., "Internet of Things (IoT): Taxonomy of security attacks", *3rd International Conference on Electronic Design*, pp. 321-326, 2016. DOI:10.1109/ICED.2016.7804660.

WEARABLE AND EMBEDDED IOT-BASED SOLUTIONS FOR BIOMEDICAL APPLICATIONS

I.S. Skarga-Bandurova, T.O. Biloborodova and A.Y. Velykzhanin

Training 1
DESIGN, ARCHITECTURE AND HARDWARE FOR REMOTE MONITORING SYSTEMS

1. Objectives and tasks

Goal and objectives: This training is an introduction to IoT wearable system for biomedical monitoring. We'll study design, architecture and hardware of IoT wearable system for biomedical monitoring. Developed wearable device for ECG monitoring will be used for ECG signal acquisition.

Learning objectives:

− study functionality elements and layers of IoT-based system for acquisition of biomedical information;

− study device hardware for ECG signal acquisition.

Practical tasks:

− acquire practical skills in health IoT-based system architecture developing;

− acquire practical skills in devices to biomedical monitoring developing;

− gather information on necessary hardware for biomedical monitoring devices;

− acquire practical skills to ECG data acquisition;

− to perform analysis to power consumption and energy efficiency of device components.

Exploring tasks:

− discover types of biomedical sensors;

− discover requirements to wearable device configuration;

− investigate IoT-based system architecture;

− analyze QRS complex of ECG signal.

Setting up

In preparation for training it is necessary:

− to clear the goals and mission of the research;

− to study theoretical material contained in this manual, and in [1-3];

− to familiarize oneself with the main procedures and specify the exploration program according to defined task.

Recommended software and resources:

Required Hardware:

− ESP-WROOM-32 DEV KIT (x1)
− OLIMEX SHIELD-EKG-EMG (x1)
− Breadboard MB-102 830 holes (x1)
− SHIELD-EKG-EMG-PRO (x1)
− ECG-GEL-ELECTRODE (x3)
− USB 2.0 Micro B Cable (x1)
− Male/Male Jumper Wires 150mm (x3)
− Poweradd Slim2 5000mAh Portable Charger Power Bank

Required Software:

− Arduino IDE 1.8.5 - https://www.arduino.cc/en/Main/Software?
− Python 2.7/3.6 - https://www.python.org/

Synopsis

In this training you will learn the main stages of designing a wireless monitoring system for biomedical information, hardware support of a wearable device for biomedical signals monitoring.

2. Brief theoretical information

The Internet of Things (IoT) is a network of physical devices and other items, embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data. Its impact on medicine will be perhaps the most important, and personal, effect. By 2020, 40% of IoT-related technology will be health-related, more than any other category, making up a $117 billion market. The convergence of medicine and information technologies, such as medical informatics, will transform healthcare as we know it, curbing costs, reducing inefficiencies, and saving lives.

Fig. 1.1 illustrates how this revolution in medicine will look in a typical IoT hospital, in practice. A patient will have an ID card that, when scanned, links to a secure cloud which stores their electronic health record vitals and lab results, medical and prescription histories. Physicians and nurses can easily access this record on a tablet or desktop computer.

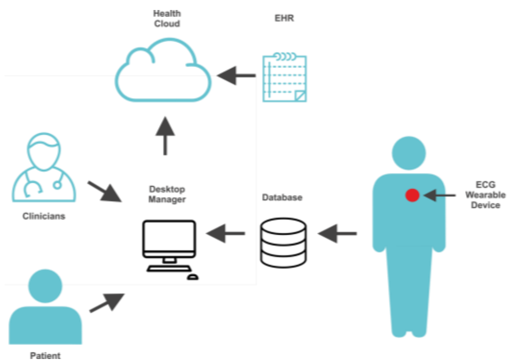

Fig. 1.1 – IoT technology for medicine domain

For some application domains, such as healthcare, the physical attributes of a sensor system are important selection criteria, particularly for body-worn configurations [1]. These attributes include weight, physical dimensions, enclosure type, sensor-mounting system, ability to wipe down, and waterproofing (that is, preventing biological fluid ingress). The weight of the sensor system is also important for mobile applications, such as those for smartphones, or in vibration applications, where the weight of the sensor could directly impact the accuracy of the measurement.

In accordance with the basic principles of work, biomedical sensors can be divided into physical, chemical and biological [2]. Classification of sensors on this principle is presented in Fig. 1.2.

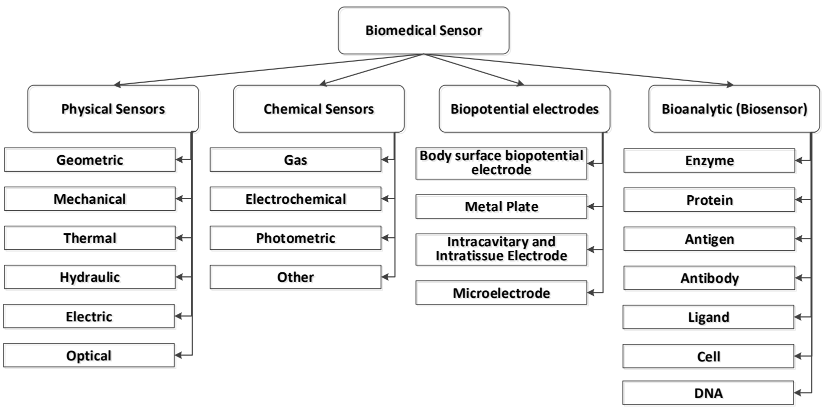

Fig. 1.2 – Classification of Biomedical Sensors

Describing of different wearable devices and sensors for health state monitoring are present in Table 1.

IoT devices and sensors have two general limitations that need to be considered when developing a biomedical information monitoring system: a small amount of memory and limited power.

When developing and using wearable biomedical devices for IoT, the following conditions should be considered:

– limited memory;
– limited energy power.

Table 1.1 – Biomedical wearable devices and sensors

Sensor	Description
Accelerometer	measures changes in the acceleration of the device caused by user's movements
Blood pressure sensor	measures systolic and diastolic blood pressures
Electrocardiogram sensor	measures the electrical activity of the heart
Electroencephalogram sensor	measures the electrical activity of the brain
Electromyogram sensor	records electrical activity produced by skeletal muscles
Glucometer	measures approximate blood glucose concentration
Galvanic skin response sensor	measures continuous variation in the electrical characteristics of the skin
Gyroscope	measures changes in device orientation caused by user's movements
Heart rate sensor	counts the number of heart contractions per minute
Magnetometer	specifics user's direction by examining the changes in the earth's magnetic field around the user
Microphone	records acoustic sounds generated by the human body (can be used for respiration analysis or emotion detection)
Near-infrared spectroscope	provides neuroimaging technology to examine an aspect of brain function
Oximeter	measures the fraction of oxygen-saturated

	hemoglobin relative to the total hemoglobin count in the blood
Pedometer	counts each step a person takes by detecting the motion of die person’s hands or hips
Respiration rate sensor	counts how many times the chest rises in a minute
Strain sensor	measures strain on different body parts (can be used to detect when the user is slouching)
Thermometer	measures an individual's body temperature

1.2.1 ECG wearable device specification

The main elements description

ESP32 functional scheme is present in Fig. 1.3.

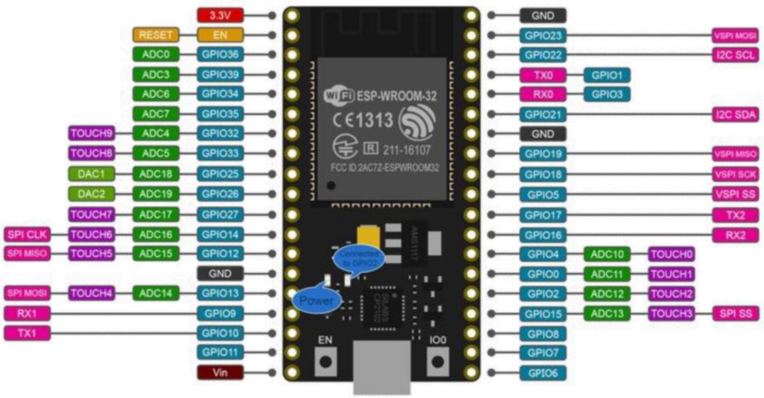

Fig. 1.3 – ESP32 functional scheme

ESP32 is a series of low cost, low power system on a chip microcontroller with integrated Wi-Fi and dual-mode Bluetooth. The ESP32 series employs a Tensilica Xtensa LX6 microprocessor in both dual-core and single-core variations and includes in-built antenna switches, RF balun, power amplifier, low-noise receive amplifier, filters, and power management modules. ESP32 is created and developed by Espressif Systems, a Shanghai-based Chinese company, and is manufactured by TSMC using their 40 nm process. It is a successor to the ESP8266 microcontroller.

SHIELD-EKG-EMG functional scheme is present in Fig. 1.4.

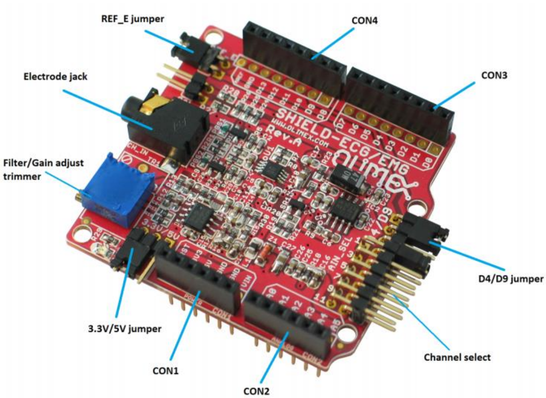

Fig. 1.4 – SHIELD-EKG-EMG functional scheme

SHIELD-EKG-EMG converts the analog differential signal (the ECG/EMG bio potentials generated by muscles), attached to its CH1_IN+/CH1_IN- inputs, into a single stream of data as output. The output signal is analog and have to be discretized further with aim to give the option of digital processing. This is done via dedicated ADC embedded in the MCU of the base board.

SHIELD-EKG-EMG's total gain is the product of the gains of each discretization stage: Instrumental Amplifier(G1=10), OAmp with regulated gain (G2=6..101) and 3rd order "Besselworth" filter (G3=3.56). Then, the Gtotal = G1*G2*G3 = 10*(6..101)*3.56. By default, we have set the G2 gain approximately ~80. Then, Gtotal = 10*(~80)*3.56 ~ 2848.

1.2.2 ECG Signal Processing Basics

ECG tracing

A typical ECG tracing of a normal heartbeat consists of a P wave, a QRS complex and a T wave. A small U wave is normally visible in 50 to 75% of ECGs. The baseline voltage of the electrocardiogram is called the isoelectric line. Fig. 1.5 beneath is the schematic of a normal ECG.

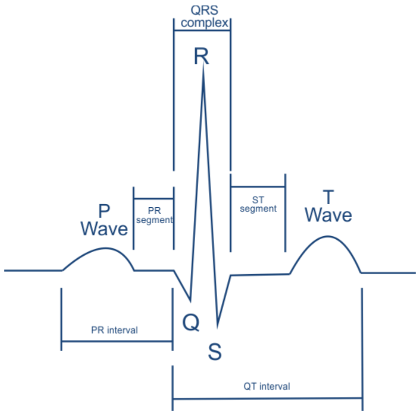

Fig. 1.5 – QRS complex schematic of a normal ECG

The frequency of a signal measures the cyclic rate or repetition, and is measured in Hertz (Hz). A frequency of 1 Hz means a signal repeat itself every one second. Our hearts produce electrical activity recorded by electrodes as a signal. The sinoatrial node fires at roughly 50 to 90 beats per minute, and for the sake of this post we will say 60 beats per minute is the happy median. This means the heart has a fundamental frequency of 1 Hz at this heart rate. Therefore, all of the ECG components (P, QRS, and T) will occur at or above this frequency.

The ECG signal is comprised of multiple sources. The recording is made through electrodes on the skin, which capture more than just the electrical activity of the heart. The primary electrical components captured are the myocardium, muscle, skin-electrode interface, and external interference.

ECG Component Frequencies

The common frequencies of the important components on the ECG:

Heart rate: 0.67 – 5 Hz (i.e. 40 – 300 bpm)

P-wave: 0.67 – 5 Hz

QRS: 10 – 50 Hz

T-wave: 1 – 7 Hz

High frequency potentials: 100 – 500 Hz

The common frequencies of the artifact and noise on the ECG:

Muscle: 5 – 50 Hz

Respiratory: 0.12 – 0.5 Hz (e.g. 8 – 30 bpm)

External electrical: 50 or 60 Hz (A/C mains or line frequency)

Other electrical: typically >10 Hz (muscle stimulators, strong magnetic fields, pacemakers with impedance monitoring).

The skin-electrode interface requires special note, as it is the largest source of interference, producing a DC component of 200-300 mV. Compare this to the electrical activity of your heart, which is in the range of 0.1 to 2 mV. The interference seen from this component is magnified by motion, either patient movement, or respiratory variation.

Heart rate data processing techniques

ECG signal processing typically includes:

– linear digital filtering - time-domain analysis;

– nonlinear transformation – frequency-domain analysis.

Heart rate variability evaluation:

– R-peak detection, beat per minutes calculating from time-domain analysis of ECG signal;

– extracting heart rate measures;

– anomaly detection.

Knowledge of the basic of signal processing helps to find new ways and methods to extract data patterns that includes signal.

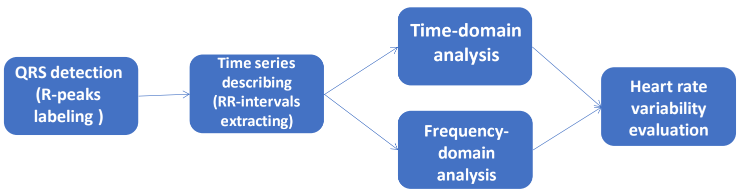

Fig. 1.6 –The general stages of heart rate variability evaluation process

3. Execution order and discovery questions

1. Assemble the EEG wearable device (see Fig. 1.7) using hardware present in Table 1.2.

Table 1.2 – ECG device components

Title	Component
ESP-WROOM-32 DEV KIT	
OLIMEX SHIELD-EKG-EMG	
Breadboard MB-102 830 holes	
SHIELD-EKG-EMG-PRO	
ECG-GEL-ELECTRODE	
USB 2.0 Micro B Cable	
Male/Male Jumper Wires 150mm	
Poweradd Slim2 5000mAh Portable Charger Power Bank	

Fig. 1.7 – The EEG wearable device

2. Download and install

2.1 Download & install python (the version that is convenient for you):

a. Install pySerial (last version).

b. Install PyQt4 (for python 2.7) or PyQt5 (for python 3.6).

c. Install pyqtgraph (last version).

2.2 Install Arduino IDE.

2.3 Using this manual, install Arduino Core for ESP-32 from https://github.com/espressif/arduino-esp32.

2.4 Update ESP32 firmware from Appendix A.

2.5 Connect ESP32 to computer and look at which COM port your device appeared on.

2.6 In python script change COM port;

3. Obtained ECG signal follow acquisition technique.

3.1 Place the electrodes on the body as follows Fig. 1.8:

– white electrode on the left arm;

– red electrode on the right arm;

– black electrode on the left leg.

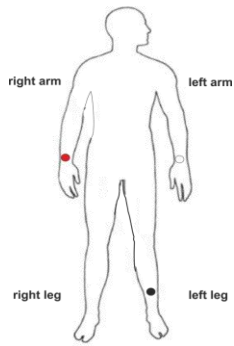

Fig. 1.8 – The electrodes location

3.2. Run python script from Appendix B (ESP 32 must be connected to your computer).

3.3 Get the ECG signal.

4. Requirements to the content of the report

Report should contain 5 sections: Introduction (I), Methods (M), Results (R), and Discussion (D)

– (I): background / theory, purpose and discovery questions

– (M): complete description of the software, and procedures which was followed in the experiment, experiment overview, figure / scheme of testing environment, procedures

– (R): narrate (like a story), tables, indicate final results;

– (D): answers on discovery questions, explanation of anomalies, conclusion / summary.

5. Test questions

1. What the biomedical sensors classification by the basic principles of work you know?
2. What are the IoT wearable device limitation?
3. What the main components of ECG wearable device?
4. How are electrodes location for ECG signal acquisition?

6. Recommended literature

1. M. J. McGrath, N. S. Cliodhna, N. Dawn, ″Sensor technologies: healthcare, wellness and environmental applications″, Apress, 2014.

2. G. Zhou, Y. Wang, L. Cui, ″Biomedical sensor, device and measurement systems″, *In Advances in Bioengineering*. Rijeka, Croatia InTech, 2015.

3. M. U. Ahmed, et al. ″Internet Of Things (IoT) Technologies for Healthcare″, Springer International Publishing, 2018.

Appendix A

```
void setup() {
    Serial.begin(115200);
}

void loop(){
    Serial.println(analogRead(A0));
    delay(7);
}
```

Appendix B

```
#!/usr/bin/python
# -*- coding: utf-8 -*-

from pyqtgraph.Qt import QtGui, QtCore
import numpy as np
import pyqtgraph as pg
from pyqtgraph.ptime import time
import serial

app = QtGui.QApplication([])

p = pg.plot()

p.setWindowTitle('ECG')
curve = p.plot()


data = [0]
raw=serial.Serial("COM6", 115200) # change to your COM
port
ptr = 0

def update():
    global curve, data, ptr
    line = raw.readline()
    data.append(int(line))
    curve.setData(data)
    curve.setPos(-(ptr+1), 0)
    ptr += 1
    app.processEvents()

timer = QtCore.QTimer()
timer.timeout.connect(update)
timer.start(0)

if __name__ == '__main__':
    import sys
    if (sys.flags.interactive != 1) or not
hasattr(QtCore, 'PYQT_VERSION'):
        QtGui.QApplication.instance().exec_()
```

Training 2
EXPLORING THE NETWORK STACK IN HEALTH IoT-BASED SYSTEMS

1. Objectives and tasks

Goal and objectives: This training is the foundation to IoT network configuration for biomedical monitoring. We'll study data channels, network hardware setting, data acquisition, and transmission technique. Configure wearable device, network hardware, and software for ECG monitoring data transmission to server and ECG signal visualization.

Learning objectives:

− study IoT network short-range and long-range communications for biomedical monitoring;

− study requirements to health IoT network hardware configuration.

Practical tasks:

− acquire practical skills in working with network hardware and software configuration for ECG signal transmission;

− acquire practical skills in software configuration for ECG signal visualization;

− gather information on existing monitoring data transmission channels.

Exploring tasks:

− discover the process of biomedical signal visualization;

− analyze requirements to network communication channel and hardware configuration;

− investigate short-range and long-range communications applying.

Setting up

In preparation for training it is necessary:

− to clear the goals and mission of the research;

− to study theoretical material contained in this manual, and in [1−3];

− to familiarize oneself with the main procedures and specify the exploration program according to the defined task.

Recommended software and resources:

Required Hardware:

− ESP-WROOM-32 DEV KIT (x1)
− OLIMEX SHIELD-EKG-EMG (x1)
− Breadboard MB-102 830 holes (x2)
− USB 2.0 Micro B Cable (x1)
− Male/Male Jumper Wires 150mm (x3)
− WiFi Router (x1)
−Poweradd Slim2 5000mAh Portable Charger Power Bank

Required Software:

−Arduino IDE 1.8.5 - https://www.arduino.cc/en/Main/Software?
−Python 2.7/3.6 - https://www.python.org/

Synopsis

In this training, you will learn IoT network short-range and long-range communications for biomedical monitoring, requirements to health IoT network hardware configuration, the process of biomedical signal visualization.

2. Brief theoretical information

One of the major challenges to implementing the IoT has to do with communication; although many devices now have sensors to collect data, they often talk with the server in their own language [1]. Manufacturers each have their own proprietary protocols, which means sensors by different makers can't necessarily speak with each other. This fragmented software environment, coupled with privacy concerns and the bureaucratic tendency to hoard all collected information, frequently maroons valuable info on data islands, undermining the whole idea of the IoT.

Communications related to the Internet of Things for healthcare can be classified into two main categories: short-range communications, and long-range communications. The former is used to communicate between devices within the wearable body area network (WBAN), whilst the latter provides a connection between the central node of the WBAN and a base station.

Short-Range Communications

In the context of wearable healthcare systems, short-range communications are often used between nodes, particularly between sensor nodes and the central node where data processing occurs. Although short-range communications standards can be used for other purposes (i.e. developing mesh networks for smart lighting), this survey focuses on the purpose of developing a small WBAN that is comprised of only a few sensors and a single central node. Many short-range communications standards exist, but perhaps the most commonly used ones in IoT are Bluetooth Low Energy and ZigBee.

Bluetooth Low Energy was developed by the Bluetooth Special Interest Group (SIG) to provide an energy-efficient standard that could be used by a coin-cell battery-operated devices, including wearables. It also aimed to enable IoT, connecting small peripheral devices to processing devices such as smartphones. Bluetooth Low Energy is used in a star topology, which is suitable for healthcare applications. The central node would act as the center of the star topology, with sensors linked to it. The sensors will have no need to communicate with each other directly. The range for Bluetooth Low Energy is 150 m in an open field; it would be much less in non-ideal conditions. It also has a low latency of 3 ms, and a high data rate of 1Mbps. The range is clearly sufficient for use in a healthcare WBAN where nodes are physically proximal, and the extremely low latency is ideal for applications such as emergency health. Bluetooth Low Energy operates in the 2.4 GHz band, a band also used by classic Wi-Fi and ZigBee. Power consumption in Bluetooth Low Energy is extremely low. With careful hardware design and low-energy programming, Bluetooth Low Energy would clearly be suitable for healthcare applications. Security has been implemented in a variety of ways for Bluetooth Low Energy. It is secure and features good range, low latency, low power consumption, and robustness to interference. This standard is highly recommended to designers, as it is currently the most suitable standard for implementation into wearable healthcare systems.

The ZigBee standard was designed by the ZigBee Alliance, specifically for providing low-cost, low power networks for M2M communications. It builds on the IEEE 802.15.4 physical standard [2]. It is commonly known as the standard for mesh networks, but it can also be used in the star topology required of a WBAN with one central node and many sensing nodes. Different ZigBee modules provide different characteristics in terms of range, data rate, and power consumption. The XBee Pro can reach up to 90 m in an urban environment, but with 63 mW of power being used to transmit. There are ZigBee-based solutions for a wide variety of applications, but for the use case of a healthcare WBAN, the XBee 1mW would be suitable. Only a small range is needed for on-body communications, so choosing the lowest-power solution is preferable. Data rates are also variable. XBee and XBee Pro have a data rate of up to 250 kbps. In a healthcare environment, it would be preferable to opt for a higher data rate, as this will reduce the latency in the system and ensure critical health data is delivered timely. ZigBee can operate at a range of frequencies, including 868MHz, 900MHz, and 2.4GHz bands, depending on the module chosen. Each of these bands faces interference. ZigBee uses CSMA-CA to reduce collisions, and implements re-transmission if messages sent are not acknowledged. Several security features are provided by ZigBee, though most are optional and must be enabled by the network developer. ZigBee's security model is largely based on 128-AES encryption and offers types of security keys - a link key, a network key, and a master key. Overall, ZigBee is reasonably well-suited to healthcare applications. It provides robustness to interference and several security mechanisms. The main drawback of using ZigBee is that key exchange can be compromised unless implemented extremely well by the manufacturer. This could pose a risk to healthcare systems where sensitive patient data is being exchanged regularly. Additionally, ZigBee is not commonly implemented in devices such as smartphones, while Bluetooth Low Energy typically is. This makes it less compatible with existing devices, and therefore it is suggested that it would be better suited to fixed-location, standalone purposes such as home automation than it is to wearable healthcare systems. It is therefore recommended that system designers prefer Bluetooth Low Energy for wearable sensors over ZigBee, particularly in applications where privacy is critical.

Long-Range Communications

Low-Power Wide-Area Networks (LPWANs) are a subset of long-range communications standards with high suitability for IoT applications [3]. The range of an LPWAN is generally several kilometers, even in an urban environment. This is significantly longer than the range of traditional IoT communications types such as Wi-Fi or Bluetooth, whose ranges are in the order of meters and thus would require extensive and costly mesh networking or similar to be plausible for healthcare. LPWANs also have a significant advantage over cellular networks such as 3G in that they are designed to support short bursts of data infrequently. This is suitable for a large number of healthcare applications, including monitoring general health and receiving hourly updates, monitoring critical health and receiving emergency calls, and rehabilitation where updates may only be necessary once daily. This design principle also allows for low-power device design, which in turn ensures that the designed healthcare devices will operate for longer before human interaction is required to recharge or change batteries. This reduces the risk of patients being offline and provides more convenience to the wearer. Based on these advantages, it is suggested that LPWANs are the best solution for transmitting data from the central node to the cloud for storage or further processing. The most prominent standards for LPWANs are Sigfox and LoRaWAN. While these standards are well-established, they face competition from emerging standards including NB-IoT.

3. Execution order and discovery questions

Instructions

1. Download and install Python (the version that is convenient for you).

1.1. Install PySerial;

1.2. Install PyQt4 (for Python 2.7); or PyQt5 (for Python 3.6);

1.3. Install pyqtgraph.

2. Install Arduino IDE.

2.1. Using this manual, install Arduino Core for ESP-32 from https://github.com/espressif/arduino-esp32.

3. Configure your router.

3.1. Wi-Fi set up;

3.2. Turn on DHCP;

4. Connect a router to your computer.

5. Edit ESP32 firmware (change IP address, SSID, password).

6. Update ESP32 firmware from Appendix A.

7. Connect ECG electrode to your body.

8. Run python script from Appendix B.

9. Get the visualized ECG signal.

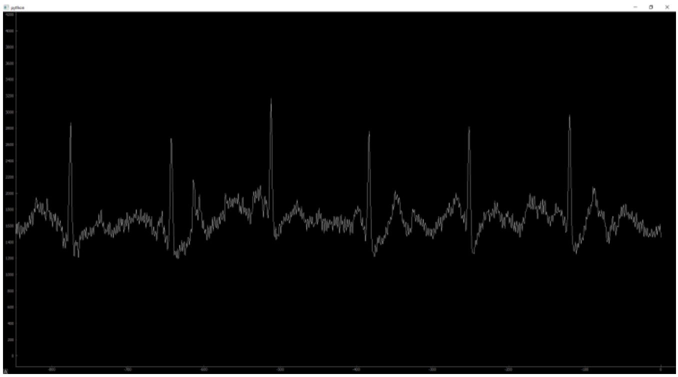

Fig. 2.1 –The visualized of obtained ECG signal

10. Right-click on plot and save data in CSV file for future work.

4. Requirements to the content of the report

Report should contain 5 sections: Introduction (I), Methods (M), Results (R), and Discussion (D)

– (I): background / theory, purpose and discovery questions

– (M): complete description of the software, and procedures which was followed in the experiment, experiment overview, figure / scheme of testing environment, procedures

– (R): narrate (like a story), tables, indicate final results;

– (D): answers on discovery questions, explanation of anomalies, conclusion / summary

5. Test questions:

1. What the range of communications for biomedical monitoring are used?
2. What the difference in applying some range of communications for biomedical monitoring?
3. What range communications are Bluetooth Low Energy, ZigBee?
4. Name ZigBee disadvantage.
5. What range communications are Sigfox, LoRaWAN?

6. Recommended literature

1. D. V. Dimitrov, ″Medical internet of things and big data in healthcare″, *Healthcare informatics research*, vol. 22, no. 3, pp.156-163.

2. Digi, ZigBee Wireless Standard, *Digi.com*, 2017. [Online]. Available: https://www.digi.com/resources/standardsand-technologies/ rfmodems/zigbee-wireless-standard. [Accessed: 30-Jul-2019].

3. S. B. Baker, et al. "Internet Of Things For Smart Healthcare: Technologies, Challenges, And Opportunities". *IEEE Access*, vol 5, 2017, pp. 26521-26544.

Appendix A

```
#include <WiFi.h>
#include <WiFiUdp.h>

/* WiFi network name and password */
const char * ssid = "*****"; // change SSID
const char * pwd = "*****"; // change password

const int udpPort = 44444;
IPAddress pcIP (192,168,1,100);
WiFiUDP udp;
String mrt = "";
void setup(){
  Serial.begin(115200);
  WiFi.begin(ssid, pwd);
  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }
  Serial.println("");
  Serial.print("Connected to ");
  Serial.println(ssid);
  Serial.print("IP address: ");
  Serial.println(WiFi.localIP());
}

void loop(){
  mrt = int(analogRead(A0));
  udpSendMessage(pcIP, mrt, udpPort);
  delay(6);
}
```

```
   bool udpSendMessage(IPAddress ipAddr, String udpMsg, int
udpPort) {
     /** WiFiUDP class for creating UDP communication */
     WiFiUDP udpClientServer;

     // Start UDP client for sending packets
     int connOK = udpClientServer.begin(udpPort);

     if (connOK == 0) {
       Serial.println("UDP could not get socket");
       return false;
     }
     udpClientServer.begin(udpPort);
     int beginOK = udpClientServer.beginPacket(ipAddr,
udpPort);

     if (beginOK == 0) { // Problem occured!
       udpClientServer.stop();
       Serial.println("UDP connection failed");
       return false;
     }
     int bytesSent = udpClientServer.print(udpMsg);
     if (bytesSent == udpMsg.length()) {
       Serial.println("Sent " + String(bytesSent) + " bytes
from " + udpMsg + " which had a length of " +
String(udpMsg.length()) + " bytes");
       udpClientServer.endPacket();
       udpClientServer.stop();
       return true;
     } else {
       Serial.println("Failed to send " + udpMsg + ", sent
" + String(bytesSent) + " of " + String(udpMsg.length()) +
" bytes");
       udpClientServer.endPacket();
       udpClientServer.stop();
       return false;
     }
   }
```

Appendix B

```
   #!/usr/bin/python
# -*- coding: utf-8 -*-

import socket
import traceback
from pyqtgraph.Qt import QtGui, QtCore
```

```
import numpy as np
import pyqtgraph as pg
from pyqtgraph.ptime import time

#assign variables n stuff
host = '0.0.0.0'
port = 44444
csvf = 'test.csv'

app = QtGui.QApplication([])

#do UDP stuff
s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
s.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
s.setsockopt(socket.SOL_SOCKET, socket.SO_BROADCAST, 1)
s.bind((host, port))

p = pg.plot()

p.setWindowTitle('live plot from serial')
curve = p.plot()

data = [0]
ptr = 0

def update():
    global curve, data, ptr
    try:
        message, address = s.recvfrom(1024)
        data.append(int(message))
        curve.setData(data)
        curve.setPos(-(ptr + 1), 0)
        ptr += 1
        app.processEvents()
    except(KeyboardInterrupt, SystemExit):
        raise
    except:
        traceback.print_exc()
timer = QtCore.QTimer()
timer.timeout.connect(update)
timer.start(0)

if __name__ == '__main__':
    import sys
    if (sys.flags.interactive != 1) or not hasattr(QtCore,
'PYQT_VERSION'):
        QtGui.QApplication.instance().exec_()
```

Training 3
ANALYSIS DATA FUSION TECHNIQUE FOR REAL-TIME BIOMEDICAL MONITORING

Goal and objectives: This training is study of approaches to biomedical monitoring data analysis. We'll study biomedical data analysis for real-time monitoring using data fusion technique.

Learning objectives:

− study technique to ARIMA model better order selection by Bayesian Information Criterion;

− study Base Probability Assignment (BPA) estimation;

− study Conflict of Probabilities estimation;

− study basic and time-series Dempster-Shaffer fusion calculation.

Practical tasks:

− acquire practical skills EEG data fusion technique;

− acquire practical skills to prediction with ARIMA model;

− gather information on prediction model;

− to perform Dempster-Shaffer theory to data analysis.

Exploring tasks:

− discover certain biomedical states using data fusion technique;

− investigate methods to biomedical data analysis.

Setting up

In preparation for training it is necessary:

− to clear the goals and mission of the research;

− to study theoretical material contained in this manual, and in [1, 2];

− to familiarize oneself with the main procedures and specify the exploration program according to defined task.

Synopsis

In this training you will learn necessary steps to real-time monitoring data fusion technique.

2. Brief theoretical information

Currently, IoT-based systems rely on algorithms that employ very simple models of the physiological signals in order to detect the correlations of interest. Often, for instance, the models are based on pre-determined thresholds of specific signal parameters. These parameters can typically be extracted through signal processing, and thus low-energy IoT-based systems has been the predominant computational approach in current biomedical devices.

Clinically relevant processes that must be detected in biomedical applications are generally physiologically complex. The ability to model these, and their manifestations in the signals that are available through chronic sensing, poses a primary challenge.

A second challenge is that that signals available through low-power chronic sensing typically represent the superposition of numerous physiological sources. Thus, the models must be able to reject these with very high specificity, usually higher than (linear) signal processing affords.

The third challenge is that efficient methods for developing and adapting the detection models are required. This can play a critical role in improving accuracy by allowing patient-specific factors to be more readily incorporated.

With respect to the challenges faced in biomedical detection applications, two important developments have recently emerged. The first is the availability of patient data in the healthcare domain, and the second the advancement of machine-learning techniques for data-analysis. Hospitals today widely employ data-bases where patient signals recorded from bedside monitors (e.g., EEG, ECG, etc.) are logged along with observational and/or diagnostic annotations. As a result, a large amount of data is available, corresponding to patients with a broad range of clinical conditions. Practices for annotating the datasets are also improving, leading to high-quality, clinically-relevant labels are being directly applied to the signals. Biomedical devices can directly take advantage of the annotated databases without the need for supplementary models to correlate with alternate signals.

Machine-learning techniques provide powerful methods for exploiting the large-scale availability of patient data. The generality of the modeling and classification methods means that they can be applied across a wide range of biomedical applications.

By treating the biomarkers as a feature vector, a machine-learning classifier can be used. Various options for machine-learning-based classification are available, and these offer the possibility to efficiently scale the models to handle a large number of features with diverse correlations.

Biomarkers, however, are closely coupled to the clinical factors, and therefore their precise choice varies from application to application. For instance, for seizure detection, information is contained in the spectral content of the patient's electroencephalograph (EEG), while for cardiac arrhythmia detection information is contained in the waveform morphology of the patient's electrocardiograph (ECG); the biomarkers are thus choosing accordingly.

Biomedical signals can also exhibit a wide range of characteristics within both the physiologic and pathophysiologic states. For instance, in the physiologic state, EEG exhibits different characteristics depending on whether an individual is awake or asleep. Similarly, in the pathophysiologic state, the EEG observed at the onset, middle, and end of a seizure may be very different. Depending on the application, however, a system may be required to differentiate between the physiologic and pathophysiologic states, or to discriminate among various sub-states within each of these two states.

Accurate physiology and chronic health evaluation is an important task in medicine. In this context, the recent cutting-edge technologies as a Big Data, Internet of Things (IoT), as well as mobile technologies, and wearable devices step-by-step take up the art of diagnostic to a new level. Data extracted from different diagnostic devices are the rich source of information. For example, data from the electroencephalogram (EEG) can be used not only in clinical research to understand the patient status and their diagnosis, but they are also heavily used in the gaming industry, IoT devices as well as for emotion recognition, military scenarios, etc. Hence, many approaches to machine classification have been proposed in this area. At the same time, when using these techniques, a number of issues associated with the implementation of multi-criteria parameters estimation in real time need to be improved. One of these issues is classifying the human biophysical state by EEG indicators. It is still unclear which machine classifier can be sufficient for clinical application when we have several monitoring data. The ability to group multiple monitoring data into a finite set of classes means that a decision must be made based on several sources of information. To analyze signal structures of very different sizes, we need to perform a multi-sensor analysis on the recorded EEG signal.

In conducting the EEG patient examination, it is often not possible to make a decision regarding their health status if only a few parameters are available. Abnormal values of a single variable do not indicate a specific state. Also, it is necessary to take into account the conflict of diagnostic signs and their values, the presence of a large amount of uncertain information. Traditionally, uncertainties are handled by probabilistic methods, such as Bayesian methods and the Dempster-Shafer (D-S) theory. An analysis of the literature has shown that using the D-S theory in classifying data has a definite advantage. In the presence of multiple, incomplete, uncertain, or redundant data, the use of elements of the D-S theory can improve the efficiency of data classification.

The technique to analyzing real-time data from several sources involves the following steps: (1) Data normalization; (2) Prediction future points; (3) Analysis of residuals; (4) Check for conflicts; (5) Data fusion using different D-S techniques.

1. Data Normalization

This is step applied for signals from different types. This step is not necessary.

Normalization of parameter values is carried out using transformations of simple Euclidean distance, since, in general case, various indicators of the human biophysical state are expressed in unequal units. The Euclidean distance E between x and y point in n-dimensional space is calculated as:

$$E(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} . \tag{3.1}$$

2. Prediction Future Points

This step is performed using the Autoregressive Integrated Moving Average (ARIMA) model [7].

a. Analysis of Residuals

Monitoring the status of n patient's indicators occurs in real time. Their measured values at time step k are defined as $Q_i(k), i = 1, 2, ..., n$. While $Pr_i(k)$ value means their predicted values obtained using the ARIMA model and the last measured values. Residuals are computed by $R_i(k) = abs(Q_i(k) - Pr_i(k))$ and $R_1(k)$, $R_2(k)$, $R_3(k)$ are rated as three residuals corresponding to the three studied indicators of the human biophysical state. The residuals of the three indicators are used as the sources of evidence for the DS fusion method, and the result of the fusion is the probability of an initial or opposite biophysical state of a person.

The Bayesian Information Criterion (BIC) is used to assess the quality of the ARIMA model for predicting the biophysical state of a person. BIC is a criterion for selecting a model from a class of parameterized models depending on a different number of parameters. To estimate the model, the method of finding the maximum of the likelihood function is usually used, the value of which can be increased by adding additional parameters.

The BIC is obtained under the assumption that the distribution of the sample belongs to the family of exponential distributions.

The model with the minimum BIC value is selected as the optimal model.

b. Calculation of Basic Probability Assignment and Conflict Resolution

The calculation of basic probability assignment (BPA) is performed using the residuals. The BPA function of a person's normal biophysical state can be determined as follows.

$$m(\{N\}) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left[-\frac{(x-\mu)^2}{F*\sigma^2} \right], \qquad (3.2)$$

where x denotes the residual of the indicator at a given time step; F is a constant; μ is the average value of the residual of the indicator of the biophysical state of a person; σ is the standard deviation of the residual indicator of the human biophysical state.

In the case of a binary classification, the probability of the opposite state.

$$m(\{C\}) = 1 - m(\{N\}). \qquad (3.3)$$

3. Check for Conflict of Probabilities

At this stage, data are checked in the presence of conflicts in probabilities. If there is no conflict the base D-S data fusion technique can be used. Otherwise, we propose to utilize the D-S fusion method for time series which combines successive time steps and the weighted average.

a. Data Fusion Using D-S Approach

Basic D-S fusion

The implementation of the basic D-S fusion method for $n > 2$ involves equations (3.4)-(3.6). For $m_1, m_2, ..., m_n$ n independent sets of BPA, the combinatorial probability fusion rule is defined as follows:

$$m(C) = m_1 \oplus m_2 \oplus ... \oplus m_n(C) = \begin{cases} 0, & C=\Phi \\ \dfrac{1}{1-K} \sum\limits_{\cap_i C_i = C} \prod\limits_{1 \le i \le n} m_i(C_i), & C \neq \Phi \end{cases} \quad (3.4)$$

where $K \in (0,1)$ is a coefficient of normalization that can be considered as a measure of conflict between two sets of evidence, Φ is an empty set. The higher the value of K, the greater the conflict between the two proofs regarding the event of interest (in our case, the opposite biophysical state of a person). A comparison of the probability K coefficient of evidence with K_c coefficient of consistency of evidence is used to determine whether the evidence is in conflict or not. The K coefficient is determined as follows.

$$K = \sum_{\cap_i C_i = \Phi} \prod_{1 \le i \le n} m_i(C_i) \quad (3.5)$$

And K_c the coefficient of the evidence consistency is determined as

$$K_c = \sum_{\cap_i C_i \neq \Phi} \prod_{1 \le i \le n} m_i(C_i) \quad (3.6)$$

Time-series D-S fusion

If there is a conflict, the calculation is carried out using successive time steps k and the weighted average method. For the merging via weighted average, the base probability m_i from equations (3.4) - (3.6) is converted to m_i^*

$$m_i^* = Crd \times m_i, \; i=1, 2, ..., n. \quad (3.7)$$

In this case, the multi-criteria combinatorial rule is determined as

$$m(C) = m_1 \oplus m_2 \oplus ... \oplus m_n(C) = \begin{cases} 0, & C=\Phi \\ \frac{1}{1-K^*} \sum_{\cap_i C_i = C} \prod_{1 \le i \le n} m_i^*(C_i), & C \ne \Phi \end{cases} , \tag{3.8}$$

where coefficient K^*

$$K^* = \sum_{\cap_i C_i = \Phi} \prod_{1 \le i \le n} m_i^*(C_i) . \tag{3.9}$$

Suppose that a probability of an opposite state is $m_{(k)} \oplus m_{k-1}(\{C\})$, where *k*, *k-1* are the current and previous time steps respectively. And this event occurred. In this case, the final result of a multi-criteria fusion is calculated using the basic fusion equations (3.4) - (3.6) at the nearest time steps *k*, *k-1*, *k-2*. If the residues from the three sensitive parameters do not conflict with each other, the basic D-S fusion method is used. Otherwise, an additional test is introduced, which can be expressed as follows:

$$\begin{aligned} & m_{Ri}(k) \oplus m_{Ri}(k-1)(\{C\}) > P \text{ and } m_{Ri}(k-1) \oplus m_{Ri}(k-2)(\{C\}) > P \\ & \text{and } m_{Ri}(k-2) \oplus m_{Ri}(k-3)(\{C\}) > P, \end{aligned} \tag{3.10}$$

where $m_{Ri}(k-j)$ denotes the probability assigned *i*-th residual, the biggest one from the three maximal residuals on the time step *k-j*, *j* = 0, 1, 2. *P* is the constant threshold used to compare the results of a fusion between two adjacent fragments of a particular human biophysical state and represents consistency of evidence. Usually, a constant threshold value is assumed to be 0.8; 0.9. If there is a sensitive parameter *i* that satisfies the above inequalities (3.10), then the following equation computed using the D-S fusion method is the probability of an opposite biophysical state:

$$m_{R\_i}(k) \oplus m_{R\_i}(k-1) \oplus m_{R\_i}(k-2)(\{C\}) . \tag{3.11}$$

If (3.10) is not met, a weighted average approach based on equations (3.8) and (3.9) are used to D-S fusion and obtaining the probability of the final event.

3. Execution order and discovery questions:

In this case we use a binary classification EEG signals with the classes “initial” and “opposite”, which determine the two biophysical states of a person, they are patient with open and closed eyes.

Instructions.

1. Download EEG data set from UCI Machine Learning Repository [1].

1.1. Select file A001SB1_1.

1.2. Detailed description EEG eye state data is given in [2].

1.3. Select EEG time series data fragment about 250 steps for next experiment.

1.4. Select three electrodes for next experiment.

2. Use ARIMA model for prediction.

2.1. Provide several predictions with different ARIMA order (highest order = 2).

2.2. Get the better ARIMA order using mean of all electrodes Bayesian Information Criterion (BIC).

2.3. Run ARIMA with the better order for each electrode data.

2.4. Get the residuals for each electrode on each time steps.

3. Calculate Base Probability Assignment (BPA).

3.1. Calculate probability for “initial” state $m(\{N\})$ for each electrode on each step follow equation (3.2).

3.1.1. Calculate the average value μ for each electrode for selecting EEG time series data fragment.

3.1.2. Calculate the standard deviation σ for each electrode for selecting EEG time series data fragment.

3.1.3. Define F =2.

3.1.4. Calculate probability for “opposite” state $m(\{C\})$ for each electrode on each step follow equation (3.3).

4. Check for Conflict of Probabilities on any step

5. In the absence of conflict on this step calculate basic D-S fusion follow equation (3.4)-(3.6)

6. Otherwise, get the test follow equation (3.10) for P=0,9

7. If the inequality is true - calculate time-series D-S fusion follow equation (3.11)

7.1. Calculate constant K^* follow equation (3.9)

7.2. Calculate fusion of BPA by two electrodes BPA follow equation (3.11)

8. Make a conclusion of the eyes state at the time step from the obtained fusion probability of eyes state.

4. Requirements to the content of the report

Report should contain 5 sections: Introduction (I), Methods (M), Results (R), and Discussion (D)

− (I): background / theory, purpose and discovery questions

− (M): complete description of the software, and procedures which was followed in the experiment, experiment overview, figure / scheme of testing environment, procedures

− (R): narrate (like a story), tables, indicate final results;

− (D): answers on discovery questions, explanation of anomalies, conclusion / summary

5. Test questions

1. What are the challenges in data modeling of IoT-based systems?
2. Why data fusion for biomedical monitoring is need?
3. Why data normalization is needed in data fusion technique?
4. Why Bayesian Information Criterion for ARIMA model is used?

6. Recommended literature

1. ″UCI Machine Learning Repository″, *Archive.ics.uci.edu*, 2019. [Online]. Available: https://archive.ics.uci.edu/ml/datasets/EEG+Eye+State. [Accessed: 20- Feb- 2019].

2. Rösler, O. and Suendermann, D., "A first step towards eye state prediction using EEG", *Proc. of the AIHLS*, 2013.

DEVICES WITH RECONFIGURABLE ARCHITECTURE FOR BIOMEDICAL IOT BASED APPLICATIONS

I.S. Skarga-Bandurova, T.O. Biloborodova and O.V. Berezhnyi

Training 1
EXPLORING THE STAGE OF SMARTPHONE APPLICATION DEVELOPMENT FOR HUMAN VITAL SIGNS MONITORING

1. Objectives and tasks

Goal and objectives: This training is exploring the stage of smartphone application development for monitoring human vital signs using smartphone sensors data.

Learning objectives:

− study configuration of smartphone IoT based application for using in IoT health monitoring;

− study requirements to smartphone IoT based application development for sensor data obtaining.

Practical tasks:

− acquire practical skills in development of smartphone application for IoT-based human vital signs monitoring;

− acquire practical skills in smartphone IoT based application configuration for monitoring of sensor data.

Exploring tasks:

− investigate the process of vital signs obtaining using smartphone IoT based application;

− analyze requirements to sensor data obtaining in smartphone.

Setting up

In preparation for training it is necessary:

− to clear the goals and mission of the research;

− to study theoretical material contained in this manual, and in [1]-[3];

− to familiarize oneself with the main procedures and specify the − exploration program according to the defined task.

Recommended software and resources:

− Android Studio - https://developer.android.com/studio/

− https://github.com/beloborodova-t/ALIOT-47.git

Synopsis

In this training, you will learn development process of smartphone IoT based application for vital signs monitoring, requirements to configuration of smartphone application.

2. Brief theoretical information

The overall structure of the mobile monitoring system includes the following elements: smartphone, cloud storage and data transmission over the Internet (see Fig.1.1).

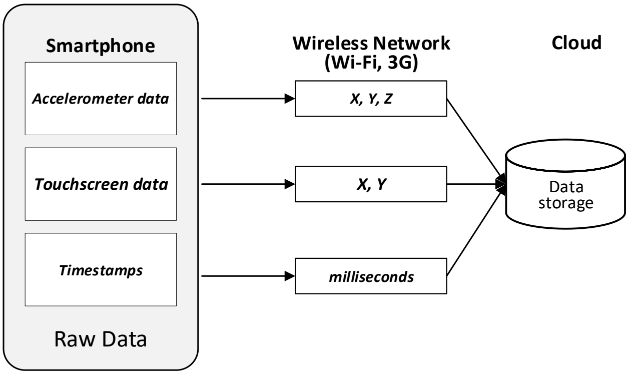

Fig. 1.1 – The architecture of personal mobile sensing system for vital signs monitoring

Constant breakthroughs in medical sensor technology and mobile devices fields, combined with growing wireless communication capabilities, have made possible the emergence of new health monitoring paradigms. A smartphone has many additional abilities like a Wi-Fi, Bluetooth, infrared, large memory and an operating system. These technologies make smartphones a personal device that is not always on but is always somewhere on us providing an always-available computing environment with many applications that can be used for continuous health state monitoring.

The minimum system requirements of the mobile application have been determined. The smartphone app module should run on Android 4.4 and higher.

3. Execution order and discovery questions

1. Download and install Android Studio.
2. Start Android Studio.
3. Create new project - Basic Activity
4. Create follow files in folder "app" → res → layout

activity_accelerometer
activity_login
content_accelerometer
content_login

5. Check creating files: right-click a folder "layout" → New → Layout resource file (see Fig. 1.1).

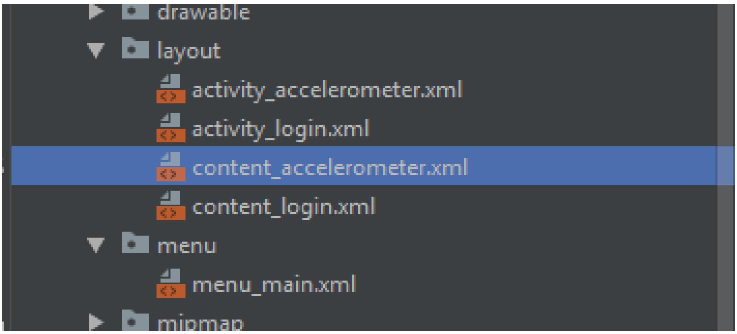

Fig. 1.1 – Checking of create files

6. Create "toolbar" in follow files: "activity_accelerometer" and "activity_login". Use menu "palette" → "container" → "AppBarLayout" (see Fig. 1.2).

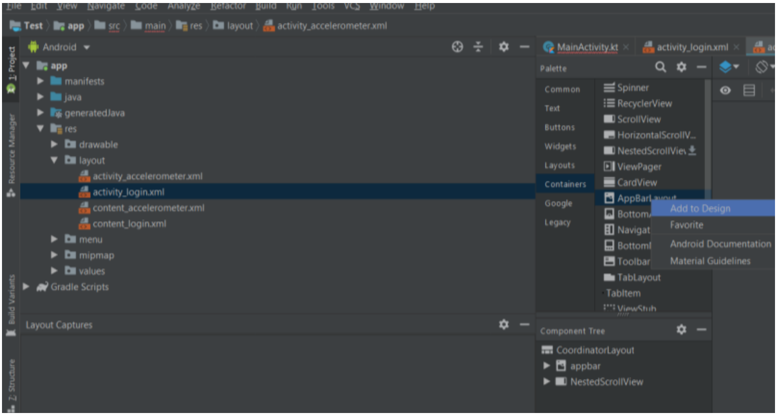

Fig. 1.2 – Toolbar creating

7. Create "include" in follow files: "activity_accelerometer" and "activity_login" with links to "content_accelerometer" and "content_login" respectively. Use menu "palette" → container → <include>.

8. Choose "content_accelerometer", use window "component tree", жмем правой кнопкой мыши по constraintLayout→ convert view→ relativeLayout→ apply (see Fig. 1.3).

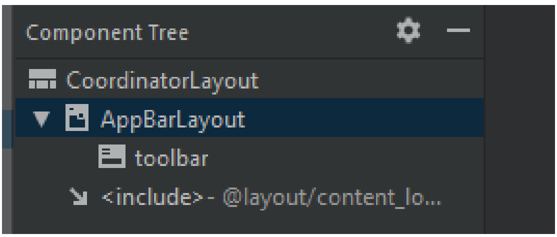

Fig. 1.3 – Component Tree window

9. Place elements from "palette" on the screen and insert text from brackets on the bottom respectively in the ID field of attributes (see Fig. 1.4).

TableLayout
    TableRow

textView (txtXLabel)
TableRow
Button (read_btn)
TableRow
LinearLayout (Layout_Graph_Container)

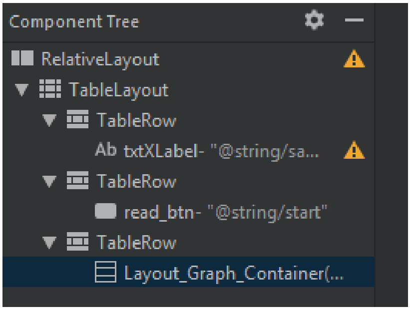

Fig. 1.4 – Component Tree of "content_accelerometer" file

10. Choose "content_login", place one button (element "button") and write "btn_login" in ID field.

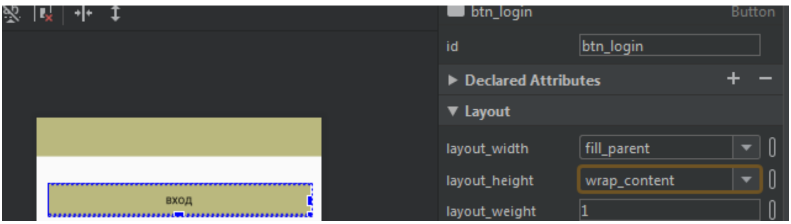

Fig. 1.5 – Button creation

11. In menu file "menu_menu" create element "item" with ID "action_logout".

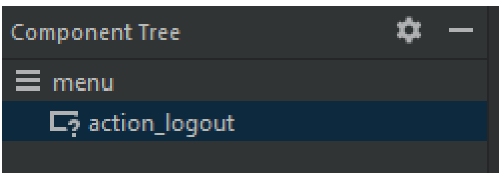

Fig. 1.6 – Creating of element "item"

12. Copy code from GitHub repository https://github.com/beloborodova-t/ALIOT-47/blob/master/pack/string.xml.txt to res → values → strings.

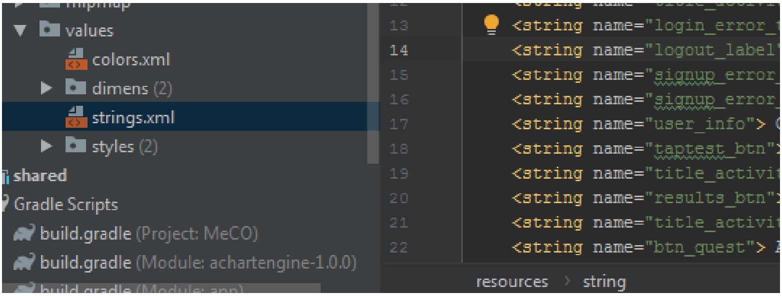

Fig. 1.7 – File configuration choosing

13. Save the project for the next training.

4. Requirements to the content of the report

Report should contain 5 sections: Introduction (I), Methods (M), Results (R), and Discussion (D)

– (I): background / theory, purpose and discovery questions

– (M): complete description of the software, and procedures which was followed in the experiment, experiment overview, figure / scheme of testing environment, procedures

– (R): narrate (like a story), tables, indicate final results;

– (D): answers on discovery questions, explanation of anomalies, conclusion / summary

5. Test questions

1. What are main elements of the mobile monitoring system?
2. What are the key elements on smartphone application interface for accelerometer data obtaining?

6. Recommended literature

1. P. Schwab, W. Karlen, "PhonePD: Learning to Diagnose Parkinson's Disease from Smartphone Data", *Arxiv.org*, 2019. [Online]. Available: https://arxiv.org/pdf/1810.01485.pdf [Accessed: 23- Feb-2019].

2. S. Arora, V. Venkataraman, A. Zhan, S. Donohue, K.M. Biglan, E.R. Dorsey, M.A. Little, "Detecting and monitoring the symptom Parkinson disease using smartphones: a pilot study", *Parkinsonism & related disorders*, vol.21, no.6, pp. 650-653.

3. J. Synnott, L. Chen, C. D. Nugent, G. Moore, "WiiPD—An approach for the objective home assessment of Parkinson's disease." *In 2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 2011, pp. 2388-2391.

Training 2
DISCOVERING SENSOR DATA TRANSMISSION USING SMARTPHONE IOT BASED APPLICATION

1. Objectives and tasks

Goal and objectives: This training is configuration of smartphone IoT based application for sensor data transmission to cloud storage and dashboard for human vital signs monitoring.

Learning objectives:

− study configuration of smartphone IoT based application for sensor data transmission;

− study configuration of cloud storage for human vital signs monitoring.

Practical tasks:

− acquire practical skills in setting of configuration of smartphone IoT based application for sensor data transmission;

− acquire practical skills in cloud storage configuration for real-time monitoring;

− gather information on existing cloud storage functions.

Exploring tasks:

− explore the configuration tools of the smartphone IoT based application to the real-time human vital signs monitoring;

− analyze cloud storage functions.

Setting up

In preparation for training it is necessary:

− to clear the goals and mission of the research;

− to study theoretical material contained in this manual, and in [1] – [3];

− to familiarize oneself with the main procedures and specify the exploration program according to the defined task.

Recommended software and resources:

− Android Studio − https://developer.android.com/studio/

− https://www.back4app.com/#

− https://github.com/beloborodova-t/ALIOT-47.git

Synopsis

In this training, you will learn configuration of smartphone IoT based application for sensor data transmission to cloud storage, the visualization of human vital signs real-time monitoring.

2. Brief theoretical information

The Back4App platform is offered as a cloud storage [1]. The platform provides the features discussed below.

Live Query function enables to subscribe to a specific query, store and synchronize app data in real-time.

JSON Import / Export function help import and export JSON files using Parse Dashboard.

The function of Manage Parse Server Versions allows ensuring full compatibility between app and server versions.

Parse Command Line Tool can be used to perform various actions on your Parse app. It can be used to create new Parse apps, deploy Cloud Code to an app, view all releases, and more.

Back4App platform allows monitoring of several users.

In order to use the system, users need only have a smartphone or tablet and Internet access to upload their data to the server. Any device that logged in with a user account can then access data from the server through Wi-Fi or a mobile data network. The system includes an Internet server that is responsible for storing and processing secure data readings.

Thus, the platform allows you to reliably track user data without significantly filling up the phone memory and using the smartphone's energy resources. The collected data is stored locally in the memory of the smartphone, and then transmitted to the server via the device, initiating an authenticated HTTP push request.

3. Execution order and discovery questions

1. Register on https://www.back4app.com/#
2. Choose «build new app».

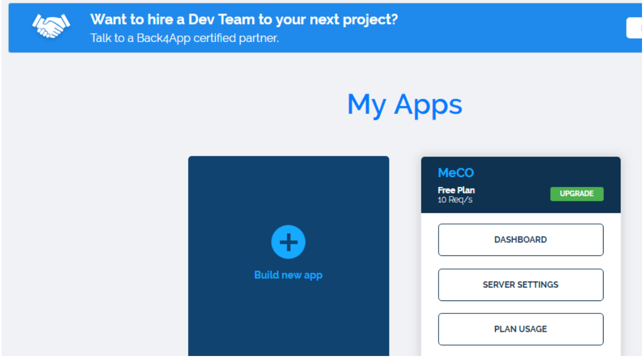

Fig. 2.1 – Building of new app

3. Go to App Setting → Security & Keys, copy key of "Application ID" and "Client key"

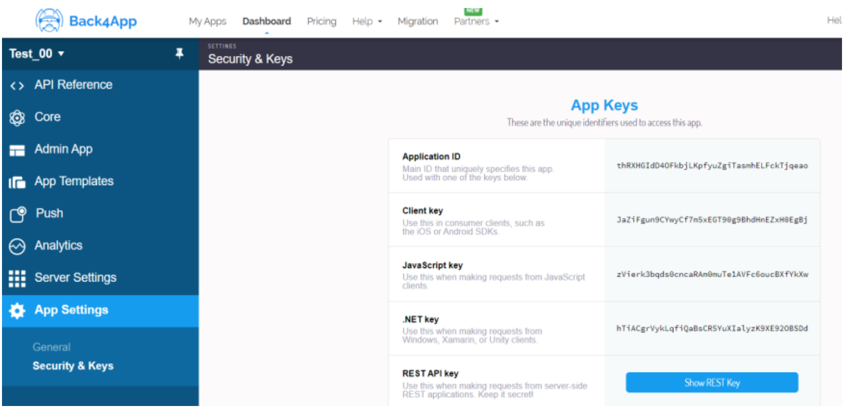

Fig. 2.2 – Obtaining of key configuration

4. Run Android Studio and open project from training 1.

5. To access the device, the Internet and the ability to data synchronize, determined the permissions in the follow file: app→ manifest→ AndroidManifest.xml. Add the following line to this file.

```
<?xml version="1.0" encoding="utf-8"?>
<manifest
xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.example.myapplication">
……
```

```
    <uses-permission
android:name="android.permission.INTERNET" />
    <uses-permission
android:name="android.permission.ACCESS_NETWORK_STATE" />
    <uses-permission
android:name="android.permission.GET_ACCOUNTS" />
    <uses-permission
android:name="android.permission.READ_PROFILE" />
    <uses-permission
android:name="android.permission.READ_CONTACTS" />
    <uses-permission android:name="android.permission.VIBRATE"
/>
  ........
```

6. Right-click on folder "Java com.example.appname", choose new → Java Class, and create follow files.

AccelAnalysis
AccelData
Login
MainActivity
ParseApp
ParseFunctions
Statistics

7. Copy the code from the corresponding .txt files into them (except for the first line) from GitHub repository https://github.com/beloborodova-t/ALIOT-47/tree/master/pack.
8. For connecting of the smartphone IoT based application and cloud storage, add the information from 3 to the ParseApp file.
9. For correct connecting of the smartphone IoT based application to cloud storage and data visualization, copy libraries from GitHub repository https://github.com/beloborodova-t/ALIOT-47/tree/master/libs into folder app → libs.
10. Write to file build.gradle(Project: appname) follow code.

```
allprojects {
    repositories {
            ...
            maven { url "https://jitpack.io" }
```

```
        }
    }
```

11. Write to the end of file build.gradle(Module:app) follow code.

```
dependencies {
        implementation 'com.github.parse-community.Parse-SDK-Android:parse:1.18.5'
    }
```

Viewing the data using a web browser is shown in Fig. 2.3.

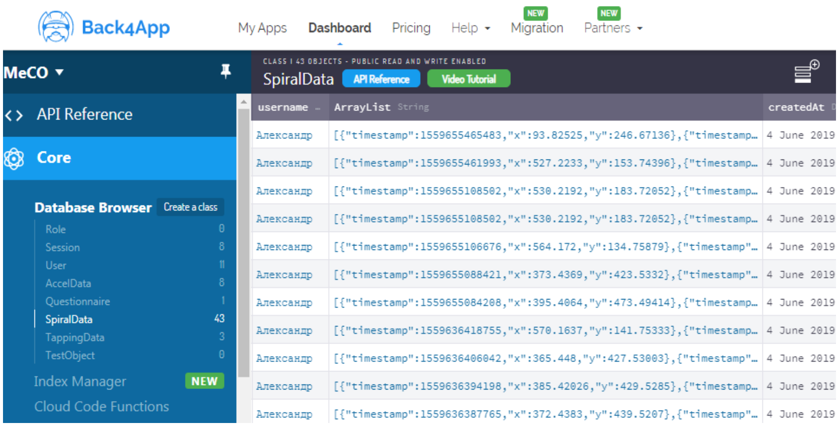

Fig. 2.3 – Vital signs data from smartphone IoT based application

4. Requirements to the content of the report

Report should contain 5 sections: Introduction (I), Methods (M), Results (R), and Discussion (D)

– (I): background / theory, purpose and discovery questions

– (M): complete description of the software, and procedures which was followed in the experiment, experiment overview, figure / scheme of testing environment, procedures

– (R): narrate (like a story), tables, indicate final results;

– (D): answers on discovery questions, explanation of anomalies, conclusion / summary

5. Test questions

1. What are the challenges in data transmission between cloud storage and smartphone application of vital signs monitoring?
2. What are the key data from cloud storage we need for smartphone configuration setting-up?

6. Recommended literature

1. P. Schwab, W. Karlen, "PhoneMD: Learning to Diagnose Parkinson's Disease from Smartphone Data", *Arxiv.org*, 2019. [Online]. Available: https://arxiv.org/pdf/1810.01485.pdf [Accessed: 23- Feb-2019].
2. S. Arora, V. Venkataraman, A. Zhan, S. Donohue, K.M. Biglan, E.R. Dorsey, M.A. Little, "Detecting and monitoring the symptom Parkinson disease using smartphones: a pilot study", *Parkinsonism & related disorders*, vol.21, no.6, pp. 650-653.
3. J. Synnott, L. Chen, C. D. Nugent, G. Moore, "WiiPD—An approach for the objective home assessment of Parkinson's disease." *In 2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 2011, pp. 2388-2391.

Training 3
REAL-TIME ACCELEROMETER DATA PROCESSING AND ANALYSIS TECHNIQUE

1. Objectives and tasks

Goal and objectives: This training is study of approaches to real-time data processing and analysis.

Learning objectives:

− study IoT network short-range and long-range communications for biomedical monitoring;

− study requirements to health IoT network hardware configuration.

Practical tasks:

− acquire practical skills in working with network hardware and software configuration for ECG signal transmission;

− acquire practical skills in software configuration for ECG signal visualization;

− gather information on existing monitoring data transmission channels.

Exploring tasks:

− discover the process of biomedical signal visualization;

− analyze requirements to network communication channel and hardware configuration;

− investigate short-range and long-range communications applying.

Setting up

In preparation for training it is necessary:

− to clear the goals and mission of the research;

− to study theoretical material contained in this manual, and in [1] – [3];

− to familiarize oneself with the main procedures and specify the exploration program according to the defined task.

Recommended software and resources:

− Weka - https://www.cs.waikato.ac.nz/ml/weka/

− https://github.com/beloborodova-t/ALIOT-47.git

Synopsis

In this training, you will learn IoT network short-range and long-range communications for biomedical monitoring, requirements to health IoT network hardware configuration, the process of biomedical signal visualization.

2. Brief theoretical information

The data processing method was proposed by calculation the statistical data parameters of the data. The next one is classifying on the basis of the calculated statistical parameters and obtaining a classification model for the next tremor detection. The data processing is carried out on a sliding window. Each window is partially overlapped with the touchscreen sampling procedure is processed separately.

For touchscreen data for each touchscreen component (X, Y measurements), the following statistical features were extracted:

1) mean;

2) standard deviation;

3) energy of the sequence: $\sum_i i^2 / w$, where *i* represents each reading and *w*= 100 - the window length;

4) Pearson's correlation between pair of touchscreen components (X-Y).

Data mining technique, such as classification, can be used on the next stage. The original and generated tremor test data set can be classified using the describing method. As a result, the confusion matrixes by classification of original and generated data sets are obtained.

The evaluation of the classification carried out using the following parameters: accuracy, sensitivity, specificity. To calculate these parameters used classification assessment by matrix confusion. Based on the matrix confusion the sensitivity, the specificity, and the accuracy are calculated as follows using true positive ς_{00}, false negative ς_{10}, true negative ς_{11} and false positive ς_{01} results of *n* observations.

$$Sensitivity = \frac{\varsigma_{00}}{\varsigma_{00} + \varsigma_{10}} * 100\%,$$

$$Specificity = \frac{\varsigma_{11}}{\varsigma_{11} + \varsigma_{01}} * 100\%,$$

$$Accuracy = \frac{\varsigma_{00} + \varsigma_{11}}{n} * 100\%.$$

3. Execution order and discovery questions

1. Download data from GitHub repository https://github.com/beloborodova-t/ALIOT-47/blob/master/Touch_data.xlsx.

2. For each component of the touch (X and Y measurements) calculate statistical parameters. The output variable is represented by three classes: (N) no tremor, (M) middle tremor, (H) heavy tremor.

3. Download and install Weka.

4. Classified original dataset using 10-fold cross-validation and Random Tree algorithm.

5. Save the obtaining result from matrix confusion.

6. Classified generated dataset using 10-fold cross-validation and Random Tree algorithm.

7. Save the obtaining result from matrix confusion.

8. Calculate sensitivity, the specificity, and the accuracy from classification model of original and generated data.

9. Compare result and make conclusion.

4. Requirements to the content of the report

Report should contain 5 sections: Introduction (I), Methods (M), Results (R), and Discussion (D)

− (I): background / theory, purpose and discovery questions

− (M): complete description of the software, and procedures which was followed in the experiment, experiment overview, figure / scheme of testing environment, procedures

− (R): narrate (like a story), tables, indicate final results;

− (D): answers on discovery questions, explanation of anomalies, conclusion / summary

5. Test questions

1. What the measures can be used for real-time data processing?
2. What the important differences between real-time and historical data analysis?
3. What the key parameters for classification accuracy estimation?

6. Recommended literature

1. P. Schwab, W. Karlen, "PhoneMD: Learning to Diagnose Parkinson's Disease from Smartphone Data", *Arxiv.org*, 2019. [Online]. Available: https://arxiv.org/pdf/1810.01485.pdf [Accessed: 23- Feb-2019].

2. S. Arora, V. Venkataraman, A. Zhan, S. Donohue, K.M. Biglan, E.R. Dorsey, M.A. Little, "Detecting and monitoring the symptom Parkinson disease using smartphones: a pilot study", *Parkinsonism & related disorders*, vol.21, no.6, pp. 650-653.

3. J. Synnott, L. Chen, C. D. Nugent, G. Moore, "WiiPD—An approach for the objective home assessment of Parkinson's disease." *In 2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 2011, pp. 2388-2391.

APPENDIX A

TEACHING PROGRAMME OF THE COURSE ITM4 "IOT FOR HEALTHCARE SYSTEMS"

DESCRIPTION OF THE COURSE

TITLE OF THE COURSE	Code
IoT for Healthcare Systems	**ITM4**

Teacher(s)	Department
Coordinating: Prof., DrS. V.S. Kharchenko **Others:** Modules ITM4.1, ITM4.2: Prof., DrS. V.S. Kharchenko, Dr. D.D. Uzun, A.A. Strielkina. Module ITM4.3: Prof., DrS. I.S. Skarga-Bandurova, Dr. T.O. Biloborodova, A.Y. Velykzhanin. Module ITM4.4: Prof., DrS. I.S. Skarga-Bandurova, Dr. T.O. Biloborodova, O.V. Berezhnyi	Computer Systems, Networks and Cybersecurity (KhAI) Computer science and Engineering (EUNU)

Study cycle	Level of the course	Type of the course
Postgraduate – for industry experts	A	Full-time tuition

Form of delivery	Duration	Language(s)
Full-time tuition	One semester	English

Prerequisites	
Prerequisites: Digital electronics, Microcontrollers, Embedded systems, Cybersecurity, System analysis, Theory of reliability, Foundations of Modeling; Programming, Telecommunications Foundations, Probability Theory and Foundations of Mathematical Statistics, Intelligent Systems	**Co-requisites (if necessary):**

Credits of the course	Total student workload	Contact hours	Individual work hours
4	120	56	64

Aim of the course: competences foreseen by the study programme
The aim of the module is to give a PhD students a deep knowledge of principles and aspects of the IoT-based technologies in healthcare and medical infrastructures: teach to analyze existing and promising technologies to model, develop, investigate, deploy and support healthcare IoT infrastructures; teach to analyze existing and promising technologies of cybersecurity and privacy providing of the healthcare IoT infrastructures; teach to developing and testing smart biomedical devices, perform real-time data analyzing; teach to developing and testing smartphone applications to vital signs monitoring, perform real-time data processing and analyzing

Learning outcomes of course	Teaching/learning methods	Assessment methods
At the end of course, the successful student will be able to: 1. Explain and discuss basic healthcare technologies based on the IoT, strategies for integrating IoT innovation into healthcare technology.	Interactive lectures, Learning in Training, Just-in-Time Teaching	Course Evaluation Questionnaire
2. Enumerate and describe main requirements of healthcare IoT standards.	Interactive lectures, Learning in Training, Just-in-Time Teaching	Course Evaluation Questionnaire
3. Describe and develop the healthcare IoT infrastructure architecture.	Interactive lectures, Learning in Training, Just-in-Time Teaching	Course Evaluation Questionnaire
4. Explain integrating of simulation models into healthcare IoT infrastructures deployment.	Interactive lectures, Learning in Training, Just-in-Time Teaching	Course Evaluation Questionnaire
5. Explain a providing communication link between the network nodes, the Internet and other medical equipment.	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Course Evaluation Questionnaire

6. Explain integrating of context-aware mechanisms for ease exploitation of the core networks' functionality.	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Course Evaluation Questionnaire
8. Compare and contrast of vital signs data acquisition approaches.	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Course Evaluation Questionnaire
9. Describe concepts, use the principles of IoT-based cloud storage.	Interactive lectures, Learning in laboratories	Course Evaluation Questionnaire
10. Explain a providing communication link between the smartphone application and healthcare cloud storage	Interactive lectures, Learning in Training, Just-in-Time Teaching	Course Evaluation Questionnaire
11. Explain integrating of context-aware mechanisms for ease exploitation of the cloud storage functionality.	Interactive lectures, Learning in Training, Just-in-Time Teaching	Course Evaluation Questionnaire

Themes	**Contact work hours**							**Time and tasks for individual work**	
	Lectures	Consultations	Seminars	Practiacl work (training)	Laboratory work	Placements	**Total contact work**	**Individual work**	**Tasks**
1. Technologies of IoT infrastructure for healthcare systems realization 1.1. Standards and requirements in IoT for health systems 1.2. Existed and	2		4				**6**	**6**	1.3. Analysis of machine learning driven healthcare Internet of Things

prospected techniques in IoT for health systems realization **Seminar:** Internet of healthcare Things: trends, problems and solutions									
2. Developing and modeling infrastructure of IoT for healthcare systems 2.1. Basic elements of the architecture of healthcare IoT infrastructure 2.2. Model range for healthcare IoT systems **Training:** Functional behavior of networked healthcare device modeling	4			3			**7**	**6**	2.3. Analysis of software tools on healthcare IoT infrastructure modeling
3 Standards and requirements for security and privacy of healthcare IoT infrastructure 3.1. Standards and requirements in IoT for health systems 3.2. Resources for managing healthcare security **Seminar:** Analysis of normative profile-generated base for security and privacy of healthcare systems	2		4				**6**	**7**	3.3. Analysis of national standards for privacy of healthcare Internet of Things
4. Security and privacy gaps according to special features of IoT infrastructure for health systems 4.1. Possible vulnerabilities and threats analysis 4.2. Possibilities of modeling of cyber security	4			3			**7**	**6**	4.3. Analysis of software tools for cybersecurity assessment of healthcare IoT

processes of healthcare IoT systems **Training:** Modeling of cyber security processes of IoT healthcare systems									
5. Biomedical sensors and data acquisition techniques 5.1 Analyzing IoT sensor data in medicine 5.2 Study of health data acquisition techniques in IoT environments **Training:** Design, architecture and hardware for remote monitoring systems	2			3			**5**	**6**	5.3 Study configuration and connection of hardware to ECG devices setting-up
6. Biomedical signal processing models for real time health data analytics 6.1 Real time tagging, aggregation, and temporal correlation **Training:** Exploring the network stack in health IoT-based systems	2			3			**5**	**6**	6.2 Research on using coupled oscillators approach in time series analysis
7. Developing and testing smart wearable devices 7.1 Embedded and wearable IoT-based systems for biomedical applications 7.2 Wearable IoT device configuration 7.3 Data analysis and prediction techniques 7.4 Cases **Training:** Analysis data fusion technique for real-time biomedical monitoring	2			3			**5**	**6**	7.5 Embedded gateway configuration 12.6 Embedded context prediction
8. IoT-based systems for remote health monitoring	2			3			**5**	**8**	8.3 Study smartphone

8.1 A Personal Mobile Sensing System for Motor Symptoms Assessment of Parkinson's Disease 8.2 Medical Aspect 8.3 Sensors and devices for Parkinson's disease assessment **Training:** Exploring the stage of smartphone application development for human vital signs monitoring									application development
9. Healthcare IoT-based systems architecture 9.1 System Architecture 9.2 Basic system components utilized and launched on the smartphone 9.3 A mobile application of the personal health monitoring system **Training:** Discovering sensor data transmission using smartphone IoT based application	2			3			**5**	**6**	9.4 Research on principles and aspects of smartphone embedded sensor
10. Healthcare IoT-based systems implementation, Results and Classification 10.1 Implementation and Results 10.2 Classification of test data **Training:** Real-time accelerometer data processing and analysis technique	2			3			**5**	**7**	10.3 Research on data obtaining technique by smartphone embedded sensor
On the whole	**24**		**8**	**24**			**56**	**64**	

Assessment strategy	Weight in %	Deadlines	Assessment criteria
Lecture activity, including fulfilling special self-tasks	10	7,14	85% – 100% Outstanding work, showing a full grasp of all the questions answered. 70% – 84% Perfect or near perfect answers to a high proportion of the questions answered. There should be a thorough understanding and appreciation of the material. 60% – 69% A very good knowledge of much of the important material, possibly excellent in places, but with a limited account of some significant topics. 50% – 59% There should be a good grasp of several important topics, but with only a limited understanding or ability in places. There may be significant omissions. 45% – 49% Students will show some relevant knowledge of some of the issues involved, but with a good grasp of only a minority of the material. Some topics may be answered well, but others will be either omitted or incorrect. 40% – 44% There should be some work of some merit. There may be a few topics answered partly or there may be scattered or perfunctory knowledge across a larger range. 20% – 39% There should be substantial deficiencies, or no answers, across large parts of the topics set, but with a little relevant and correct material in places. 0% – 19% Very little or nothing that is correct and relevant.
Learning in laboratories	30	7,14	85% – 100% An outstanding piece of work, superbly organized and presented, excellent achievement of the objectives, evidence of original thought. 70% – 84% Students will show a thorough understanding and appreciation of the material, producing work without

			significant error or omission. Objectives achieved well. Excellent organization and presentation. 60% – 69% Students will show a clear understanding of the issues involved and the work should be well written and well organized. Good work towards the objectives. The exercise should show evidence that the student has thought about the topic and has not simply reproduced standard solutions or arguments. 50% – 59% The work should show evidence that the student has a reasonable understanding of the basic material. There may be some signs of weakness, but overall the grasp of the topic should be sound. The presentation and organization should be reasonably clear, and the objectives should at least be partially achieved. 45% – 49% Students will show some appreciation of the issues involved. The exercise will indicate a basic understanding of the topic, but will not have gone beyond this, and there may well be signs of confusion about more complex material. There should be fair work towards the laboratory work objectives. 40% – 44% There should be some work towards the laboratory work objectives, but significant issues are likely to be neglected, and there will be little or no appreciation of the complexity of the problem. 20% – 39% The work may contain some correct and relevant material, but most issues are neglected or are covered incorrectly. There should be some signs of appreciation of the laboratory work requirements. 0% – 19% Very little or nothing that is

			correct and relevant and no real appreciation of the laboratory work requirements.
Course Evaluation Quest	60	8,16	The score corresponds to the percentage of correct answers to the test questions

Author	Year of issue	Title	No of periodical or volume	Place of printing. Printing house or internet link
Compulsory literature				
J. Hofdijk; B. Séroussi; C. Lovis; F. Ehrler; F. Sieverink; A. Ugon; M. Hercigonja-Szekeres	2016	Transforming Healthcare with the Internet of Things (Studies in Health Technology and Informatics)		IOS Press
Subhas C. Mukhopadhyay (Eds.)	2015	Wearable Electronics Sensors: For Safe and Healthy Living	1	Springer International Publishing. Smart Sensors, Measurement and Instrumentation
C.I. Reis; M. da S. Maximiano	2016	Internet of Things and Advanced Application in Healthcare		Medical Information Science Reference
C. Bhatt; N.Dey; A. S. Ashour	2017	Internet of Things and Big Data Technologies for Next Generation Healthcare		Springer International Publishing
S.Li; Li Da Xu	2017	Securing the Internet of Things		Syngress
S.P.Amaraweera; M.N. Halgamuge	2019	Internet of Things in the Healthcare Sector: Overview of Security and Privacy Issues		Springer International Publishing
L. Zhu; Z.Zhang; C.Xu	2017	Secure and Privacy-	1	SpringerBriefs in Signal Processing

		Preserving Data Communication in Internet of Things		
J. Cao, X. Liu	2016	Wireless Sensor Networks for Structural Health Monitoring	1	Springer International Publishing. SpringerBriefs in Electrical and Computer Engineering
D.T. Huei Lai; M. Palaniswami; R.Begg	2013	Healthcare Sensor Networks: Challenges Toward Practical Implementation		CRC Press: Hoboken
Additional literature				
R. Gravina; C.E. Palau; M. Manso,; A. Liotta; G. Fortino	2017	Integration, Interconnection, and Interoperability of IoT Systems	1	Springer International Publishing
R. Cornet; L. Stoicu-Tivadar; A. Hörbst; C. L. P. Calderón; S. K. Andersen; M. Hercigonja-Szekeres (Eds.)	2015	Studies in Health Technology and Informatics	Volume 210	IOS Press; Proceedings of the 26th Medical Informatics in Europe Conference (MIE2015) http://ebooks.iospress.nl/volume/digital-healthcare-empowering-europeans-proceedings-of-mie2015
I. Nikolaevskiy, D. Korzun, A. Gurtov	2014	Security for medical sensor networks in mobile health systems		A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th

				International Symposium on. IEEE, 2014.
J. Westin, S. Ghiamati, M. Memedi; D. Nyholm; A. Johansson; M. Dougherty; T. Groth	2010	A new computer method for assessing drawing impairment in Parkinson's disease		Journal of neuroscience methods
R.I. Griffiths; K. Kotschet; S. Arfon; Z.M. Xu, W. Johnson; J. Drago; A. Evans; P. Kempster; S. Raghav; M.K. Horne	2012	Automated assessment of bradykinesia and dyskinesia in Parkinson's disease		Journal of Parkinson's disease

АНОТАЦІЯ

УДК 004.415/.416::61](076.5)=111

Харченко В.С., Скарга-Бандурова І .С., Білобородова Т.О., Узун Д.Д., Стрєлкіна, А.А., Ілляшенко О.О., Великжанін А.Ю., Бережний О.В. **Інтернет речей для медичних систем. Тренінги** / За ред. В.С. Харченка, І.С. Скарги-Бандурової. – МОН України, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ». – 93 с.

Викладено матеріали тренінгової частини курсу ITM4 "IoT для медичних систем", підготовленого в рамках проекту ERASMUS+ ALIOT "Internet of Things: Emerging Curriculum for Industry and Human Applications" (573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP).

Наведена структура робіт з перевірки знань з курсу, відповідний тренінговий матеріал, приклади виконання завдань та критерії оцінювання. В процесі навчання наводяться теоретичні аспекти IoT для медичних систем. Вивчаються структури, моделі та технології розробки медичних IoT систем, сучасні методики і засоби проектування, модернізації та впровадження медичних IoT систем, а також розробка та апаратна оптимізація компонент IoT пристроїв в медичних системах.

Призначено для інженерів, розробників та науковців, які займаються розробкою та впровадженням IoT для медичних систем, для аспірантів університетів, які навчаються за напрямом IoT систем, а також для викладачів відповідних курсів.

Бібл. – 37, рисунків – 24, таблиць – 5, формул – 11.

ЗМІСТ

CONTENTS

Харченко Вячеслав Сергійович, Скарга-Бандурова Інна Сергіївна,
Білобородова Тетяна Олександрівна, Стрєлкіна Анастасія Андріївна,
Ілляшенко Олег Олександрович, Великжанін Артем Юрійович,
Бережний Олександр Віталійович

ІНТЕРНЕТ РЕЧЕЙ ДЛЯ МЕДИЧНИХ СИСТЕМ

Тренінги

(англійською мовою)

Редактори: Харченко В.С., Скарга-Бандурова І.С.

Комп'ютерна верстка
В.С. Харченко,
О.О. Ілляшенко,
А.А. Стрєлкіна

Зв. план, 2019
Підписаний до друку 22.08.2019
Формат 60x84 1/16. Папір офс. No2. Офс. друк.
Умов. друк. арк. 5,34. Уч.-вид. л. 5,75. Наклад 150 прим.
Замовлення 220819-1

Національний аерокосмічний університет ім. М. Є. Жуковського
"Харківський авіаційний інститут"
61070, Харків-70, вул. Чкалова, 17
http://www.khai.edu

Випускаючий редактор: ФОП Голембовська О.О.
03049, Київ, Повітрофлотський пр-кт, б. 3, к. 32.
Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції
серія ДК No 5120 від 08.06.2016 р.

Видавець: ТОВ «Видавництво «Юстон»
01034, м. Київ, вул.. О. Гончара, 36-а, тел.: +38 044 360 22 66
www.yuston.com.ua
Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції
серія ДК No 497 від 09.09.2015 р.