UNIVERSIDADE DA BEIRA INTERIOR
Faculdade de Engenharia
Departamento de Informática

Performance Assessment of Security Mechanisms for Cooperative Mobile Health Applications

Fábio Alexandre Afonso Canelo

Submitted to the University of Beira Interior in candidature for the Degree of Master of Science in Informatics Engineering

Supervised by Prof. Dr. Joel José Puga Coelho Rodrigues

Departamento de Informática
University of Beira Interior
Covilhã, Portugal
http://www.di.ubi.pt

This work has been partially supported by the *Instituto de Telecomunicações*, Next Generation Networks and Applications Group (NetGNA), Portugal, by National Funding from the FCT – *Fundação para a Ciência e Tecnologia* through the Pest-OE/EEI/LA0008/2011, and by the AAL4ALL (Ambient Assisted Living for All), project co-financed by the European Community Fund FEDER through COMPETE – *Programa Operacional Factores de Competitividade*.

Acknowledgements

First of all, I would like to thank Prof. Joel José Puga Coelho Rodrigues for giving me the chance to join the Next Generation Networks and Applications Research Group (NetGNA), for all the constant words of encouragement and for supervising my Master's thesis. The last year was undoubtedly very important in my evolution as Informatics Engineer and Person as well.

I am most grateful to the University of Beira Interior, the *Instituto de Telecomunicações*, Next Generation Networks and Applications Group (NetGNA), Covilhã Delegation, Portugal, and SAPO – Portugal Telecom for allowing me to work on this project with them.

Many thanks to all members of NetGNA, particulary Bruno Silva, Ivo Lopes, Edgar Horta, Joel Fernandes, João Dias, João Isento, and Pedro Rosa.

And of course, an enormous thanks to my family for their constant support and for all words of motivation.

Abstract

Mobile health (m-Health) applications aim to deliver healthcare services through mobile applications regardless of time and place. An m-Health application makes use of wireless communications to sustain its health services and often providing a patient-doctor interaction. Therefore, m-Health applications present several challenging issues and constraints, such as, mobile devices battery and storage capacity, broadcast constraints, interferences, disconnections, noises, limited bandwidths, network delays, and of most importance, privacy and security concerns.

In a typical m-Health system, information transmitted through wireless channels may contain sensitive information such as patient's clinic history, patient's personal diseases information (e.g. infectious disease as HIV - *h*uman immunodeficiency virus). Carrying such type of information presents many issues related to its privacy and protection.

In this work, a cryptographic solution for m-Health applications under a cooperative environment is proposed in order to approach two common drawbacks in mobile health systems: the data privacy and protection. Two different approaches were proposed: *i*) DE4MHA that aims to guarantee the best confidentiality, integrity, and authenticity of m-health systems users data and *ii*) eC4MHA that also focuses on assuring and guarantying the m-Health application data confidentiality, integrity, and authenticity, although with a different paradigm. While DE4MHA considers a peer-to-peer node message forward, with encryption/decryption tasks on each node, eC4MHA focuses on simply encrypting data at the requester node and decrypting it when it reaches the Web service. It relays information through cooperative mobile nodes, giving them the only strictly required information, in order to be able to forward a request, until it reaches the Web service responsible to manage the request, and possibly answer to that same request. In this sense, the referred solutions aim any mobile health application with cooperation mechanism embedded. For test purposes a specific mobile health application, namely SapoFit, was used. Cryptographic mechanisms were created and integrated in SapoFit application with built in cooperation mechanisms. A performance evaluation of both approaches in a real scenario with different mobile devices is performed and presented in this work. A comparison with the performance evaluations of both solutions is also presented.

Keywords

Mobile Health, m-Health, Mobile computing, Cryptography, Cooperation, Healthcare Application.

Contents

Acknowledgements i

Abstract iii

Keywords v

Contents vii

List of Figures..xi

Acronyms xiii

1. Introduction...1

1.1. Focus 1

1.2. Problem Definition...6

1.3. Objectives 6

1.4. Main Contributions...7

1.5. Dissertation Structure 8

2. Related Work 11

2.1. Mobile health (m-Health).. 12

2.1.1. Electronic Health Records 16

2.1.2. Health Level Seven International (HL7) 17

2.2. e-Health data privacy and protection 20

2.3. An Overview of Cryptographic Approaches......................... 23

2.3.1. Confidentiality.. 23

2.3.2. Integrity 25

2.3.3. Authenticity 26
2.4. Summary 27
3. Requirement Analysis 29
3.1. Essential Requirements 30
3.2. Behavioural Diagrams 30
3.2.1. Use Case Diagrams 31
3.2.2. Activity Diagrams 31
3.3. Interaction Diagrams 33
3.3.1. Sequence Diagrams 34
3.4. Used Technologies 36
3.5. Android Platform 37
3.6. Summary 39
4. Ubiquitous Cryptographic Solutions 41
4.1. Cooperation Mechanisms 41
4.2. Data Encryption for Mobile Health Applications (DE4MHA)..... 45
4.2.1. Public Key Message 47
4.2.2. Session Key Message 48
4.2.3. Symmetric Algorithm Choice 50
4.2.4. Asymmetric Algorithm Choice 52
4.2.5. Integrity and Authenticity 52
4.3. Enhanced Cryptography Solution for m-Health Applications in Cooperative Environments (eC4MHA) 53
4.3.1. Assuring Data Confidentiality 53
4.3.2. Integrity and Authenticity 55
4.3.3. Key Management 56
4.4. Summary 57
5. Performance Evaluation and System Validation 59
5.1. SapoFit Application 59
5.2. M-Health Network Scenario 60
5.3.Performance Evaluation of DE4MHA and eC4MHA 63

5.3.1. DE4MHA Performance Analysis 63

5.3.2. eC4MHA Performance Analysis 66

5.3.3. DE4MHA and eC4MHA Comparison 67

5.4. Summary 69

6. Conclusions and Future Work 71

6.1. Conclusions 71

6.2. Future Work 73

References 75

Appendix .... A

List of Figures

FIGURE 1 - GENERAL MOBILE HEALTH SYSTEM ARCHITECTURE. 2
FIGURE 2 – ILLUSTRATION OF A COOPERATION SCENARIO. 4
FIGURE 3 – ILLUSTRATION OF A TYPICAL EHR MOBILE SYSTEM ARCHITECTURE. 16
FIGURE 4 - HL7 HISTORY. 18
FIGURE 5 – ILLUSTRATION OF AN HL7 INTERFACE MODEL. 19
FIGURE 6 – GENERAL SYMMETRIC ALGORITHMS PROCESSING SEQUENCE. 24
FIGURE 7 - DIGITAL SIGNATURE. 27
FIGURE 8 - APPLICATION USE CASE DIAGRAM. 31
FIGURE 9 - DE4MHA ACTIVITY DIAGRAM. 32
FIGURE 10 - EC4MHA ACTIVITY DIAGRAM. 33
FIGURE 11 – DE4MHA SEQUENCE DIAGRAM. 34
FIGURE 12 - EC4MHA SEQUENCE DIAGRAM. 35
FIGURE 13 - ANDROID OS ARCHITECTURE. 37
FIGURE 14 – ILLUSTRATION OF THE COOPERATIVE LIST. 42
FIGURE 15 - ILLUSTRATION OF THE INTERACTION FOR AN M.HEALTH APPLICATION WITH THE COOPERATION APPROACH FOR 4 USERS. 44
FIGURE 16 - DATA EXCHANGE SEQUENCE. 47
FIGURE 17 - PUBLIC KEY MESSAGE. 48
FIGURE 18 - SESSION KEY MESSAGE. 49
FIGURE 19 - AVERAGE TIME ENCRYPTION. 51
FIGURE 20 - AVERAGE TIME DECRYPTION. 51
FIGURE 21 - ILLUSTRATION OF KEY EXCHANGE SEQUENCE ON EC4MHA. 54
FIGURE 22 - EC4MHA TYPICAL WORKFLOW. 56
FIGURE 23 - THREE MAIN ACTIVITIES SCREENSHOTS OF SAPOFIT APPLICATION: LOGIN, PLANS, AND USER PROFILE. 60
FIGURE 24 - ILLUSTRATION OF THE NETWORK SCENARIO FOR PERFORMANCE EVALUATION OF THE EC4MHA... 61
FIGURE 25 - MOBILE DEVICES USED FOR TRIALS WITH THE SAPOFIT M-HEALTH APPLICATION. 62
FIGURE 26 - SERVICE DELIVERY PROBABILITY WITH AND WITHOUT DE4MHA. 64
FIGURE 27 - SERVICE AVERAGE DELAY WITH AND WITHOUT DE4MHA. 64
FIGURE 28 - SERVICE DELIVERY PROBABILITY WITH AND WITHOUT EC4MHA. 66
FIGURE 29 - SERVICE AVERAGE DELAY WITH AND WITHOUT EC4MHA. 67
FIGURE 30 - SERVICE AVERAGE DELAY WITH DE4MHA AND EC4MHA. 68
FIGURE 31 - SERVICE DELIVERY PROBABILITY WITH DE4MHA AND EC4MHA. 69

Acronyms

3DES	:	Triple Data Encryption Standard
ACT	:	Achieved Cooperation Time
ADT	:	Android Developer Tools
AES	:	Advanced Encryption Standard
ANSI	:	American National Standards Institute
API	:	Application Programming Interface
BAN	:	Body Area Network
BMI	:	Body Mass Index
BMR	:	Basal Metabolic Rate
BT	:	Bluetooth
CATV	:	Cable Television
CDA	:	Clinical Document Architecture
CFB	:	Cipher Feedback Mode
CSCW	:	Computer Supported Cooperative Work
CWS	:	Cooperative Web Service
DE4MHA	:	Data Encryption for Mobile Health Applications
DES	:	Data Encryption Standard
DSA	:	Digital Signature Algorithm
DVM	:	Dalvik Virtual Machine
eC4MHA	:	Enhanced Cryptography Solution for Mobile Health Applications
EHR	:	Electronic Health Record
GPS	:	Global Positioning System
HL7	:	Health Level seven

HTTP	:	Hypertext Transfer Protocol
HTTPs	:	Hypertext Transfer Protocol
IDE	:	Integration Development Environment
IDEA	:	International Data Encryption Algorithm
IIHI	:	Individually Identifiable Health Information
JCA	:	Java Cryptography Architecture
JMIR	:	Journal of Medical Internet Research
JSE	:	Java Cryptography Extension
JSP	:	Java Server Pages
MD5	:	Message Digest 5
NCM	:	Node Control Message
NetGNA	:	Next Generation Networks and Applications Group
OMG	:	Object Management Group
OS	:	Operating System
PGP	:	Pretty Good Privacy
PHR	:	Personal Health Record
PKM	:	Public Key Message
RBAC	:	Role-Based Access Control
RC4	:	Rivest Cipher 4
RCM	:	Requester Control Message
REST	:	Representational State Transfer
RIM	:	Reference Information Model
RL	:	Reputation List
RN	:	Requester Node
RSA	:	Rivest Shamir Adleman
SAML	:	Security Assertion Markup Language
SDK	:	Software Development Kit
SHA-1	:	Secure Hash Algorithm 1
SKM	:	Session Key Message
SOA	:	Service Oriented Architecture
SSL	:	Secure Socket Layer
UML	:	Unified Modelling Language

WBAN	:	Wireless Body Area Network
WLAN	:	Wireless Local Area Network
WS	:	Web Service
XACML	:	eXtensible Access Control Markup Language
XML	:	eXtended Markup Language

1. Introduction

1.1. Focus

Health telematics remains as a central point in everyday society’s life and its importance has an enormous impact on people daily life. The need to provide health services regardless time and place has being increasing the mobile health applications growth and dissemination, changing many social and medical realities [1]. Currently, mobile computing faces a new trend in electronic health, due to the remarkable growing of ubiquity services, presenting never before given opportunities [2]. It has coming to offer more accessible and affordable healthcare solutions to patients that live in remote rural areas, that travel constantly or that are physically incapacitated [3], with particular incidence in developing countries [4]. Hence, health telematics are becoming a major improvement in patient’s lives, especially those who are disabled, elderly and chronically ill. Telemedicine includes the use of medical information, also known as Electronic Health Records (EHR), exchanged electronically to improve the patient’s health status [5]. This growing was analogue to the rapidly evolution of IT infrastructures and rapid access to patient data. The Web 2.0 concept and the emerging Web 3.0 is offering to healthcare professionals opportunities never given before [6]. For instance, physicians can now share medical videos (YouTube), photos (Flickr), and presentations (Slideshare), use blogs for posting medical cases and images, share hospital management information, use social networking to share ideas and tasks as well use rich site summary (RSS) feeds to keep track of alerts on their specific interests. With the advent of mobile communications supported on smart mobile devices that uses 3G and 4G mobile networks for data transport, mobile computing has been the main attraction of research and business communities. Thus, they offer countless opportunities to create efficient mobile health solutions. Mobile health (m-Health) appears as the new edge on healthcare innovation and may be defined as the integration and utilization of health services in mobile technologies. It proposes to deliver healthcare anywhere and anytime, surpassing geographical, temporal, and even organizational barriers [7], [8]. Laxminarayan and Istepanian defined mobile health for the first time, in 2000, as the "unwired e-med". In 2003, the term "m-Health" was defined as "emerging mobile communications and network technologies for healthcare systems" [9]. Figure 1 illustrates a typical mobile health system architecture, containing one or more monitoring and/or surveillance devices, such as mobile devices or wearable sensors, which should be connected to the Internet to allow information forwarding and storage.

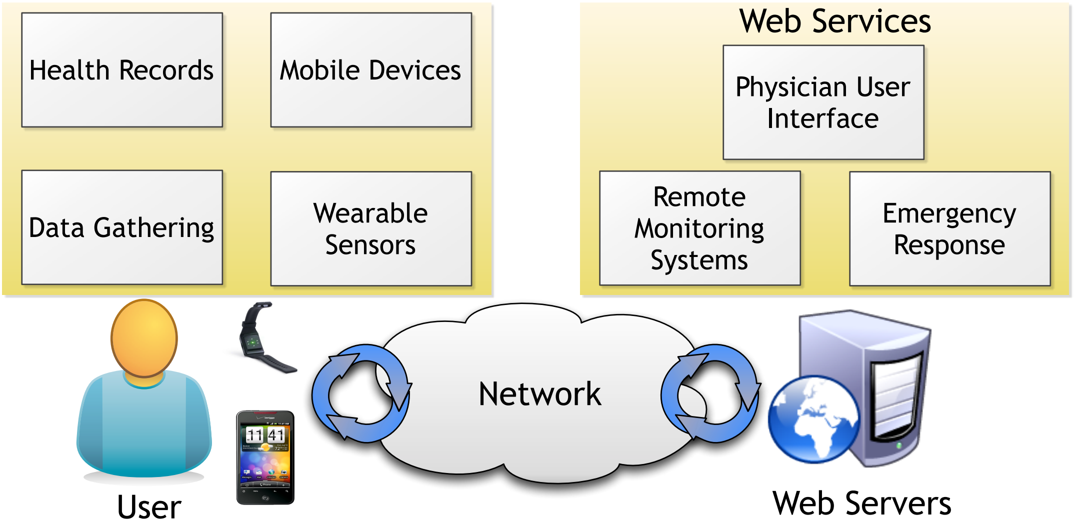


Figure 1 - General mobile health system architecture.

Laxminarayan *et al.* [10], in 2006, presents a comprehensive study about the impact of mobility on the existing e-Health commercial telemedical systems. Furthermore, it served as a basis for future m-Health technologies and services [11]. Several research topics related to health have gathered important findings and contributions from m-Health, such as, cardiology [12]-[14], diabetes [15], [16], obesity [17], [18], smoking cessation [19], among others. In the above-mentioned medical issues, m-Health applications are applied for health monitoring, diseases prevention and detection, and, in more advanced services, also provide basic diagnosis. M-Health services are also becoming popular in developing countries [4], [20] where healthcare facilities are frequently remote and/or inaccessible. However, architectures based on mobile devices and wireless communications present several challenged issues and constraints, such as, battery and storage capacity, broadcast constraints, interferences, disconnections, noises, limited bandwidths, and network delays [21]. Research studies present cooperation-based approaches as a solution to solve such limitations and also to improve wireless networks performance [22], [23].

In the healthcare context, cooperation among healthcare professionals has been studied and concluded that can improve their work and performance. Computer-supported cooperative work (CSCW) is typically used to share information through broadband and telecommunication networks (e-Mail or instant messaging) [24]. However, CSCW applied to healthcare information systems could enable patients and healthcare professionals to work together and share more efficiently health information even from remote locations [25], [26].

In this sense, cooperation-based approaches [27], [28] are presented as a solution to solve such limitations, focusing on increasing network connectivity, communication rates and reliability. Hence, a cooperation strategy regarding m-Health applications has been proposed in [27]. It essentially focuses on forwarding and retrieving data to/from nodes that have no direct connection to an m-Health application as may be seen in

Figure 2. Thus, devices without Internet connection can use m-Health applications without problems.

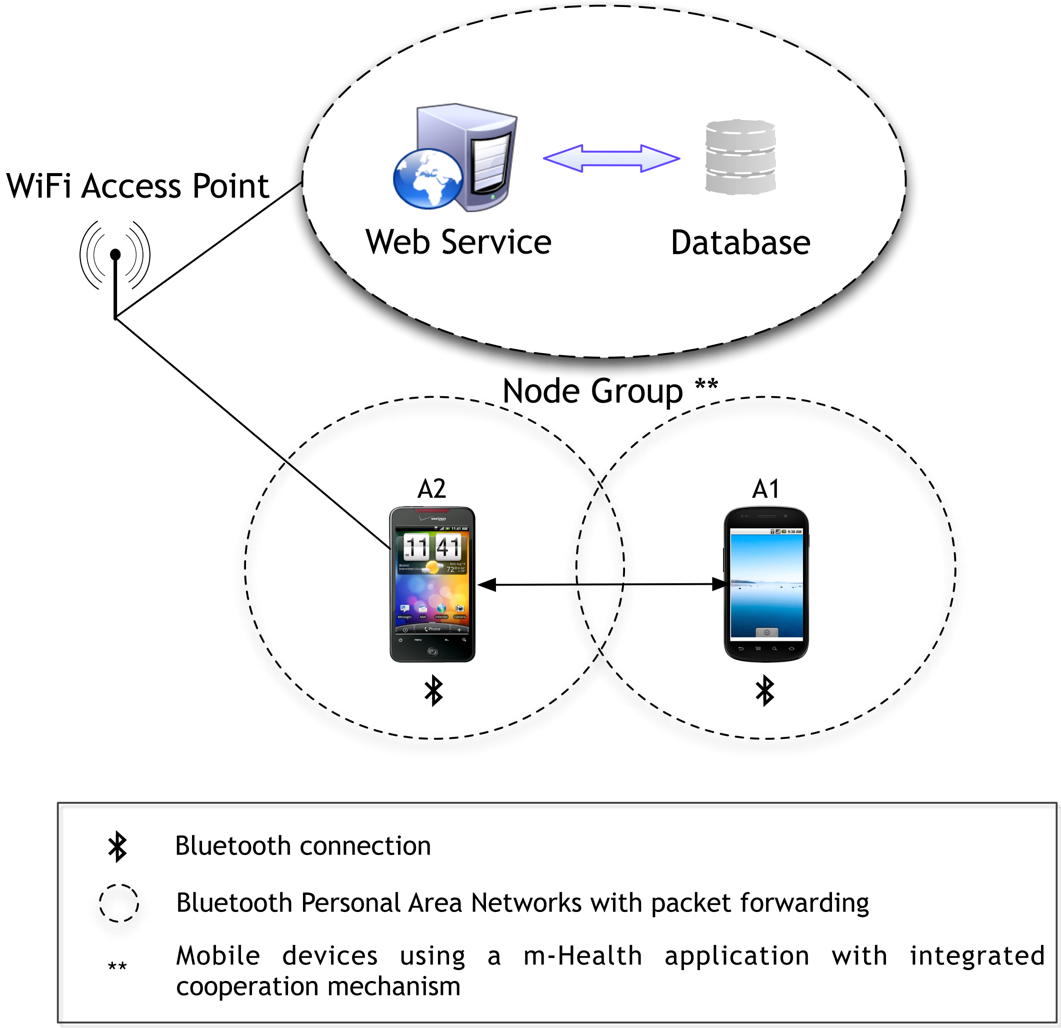

WiFi Access Point
Web Service
Database
Node Group **
A2
A1
Bluetooth connection
Bluetooth Personal Area Networks with packet forwarding
** Mobile devices using a m-Health application with integrated cooperation mechanism

Figure 2 - Illustration of a cooperation scenario.

Cooperation among mobile nodes may carry sensitive data, e.g., an application connected to a hospital monitoring vital signs of a patient or an application with diagnosis capabilities, represent scenarios where sensitive information carried by mobile nodes, through cooperation, in the network until it reaches its final destination, may possibly be compromised due to available vulnerabilities in such cooperation mechanisms. Therefore, cooperation among mobile nodes raises issues regarding user's health data privacy and protection. Furthermore, with the existence and dissemination of mobile devices as well as the high increase of health applications designed for mobile devices, currently brings issues that should be carefully addressed.

Advances in mobile health data exchange are currently being developed by Health Level Seven International (HL7), mobile health working group [29]. It creates and promotes health information technology standards and frameworks for mobile health, focusing on how data should be structured and properly secured for transmission over the network. However, and despite the efforts, this working group is still on an early stage of standards development, resulting in a lack of official standards for commercial use. In this sense, cryptographic algorithms are presented as an alternative and at the same time as a solution to the above mentioned security concerns. Due to the advent and evolution of current mobile devices, cryptographic algorithms are now capable of accomplishing its tasks without the concern of mobile resources that could decrease the overall efficiency and effectiveness of the network, degrading the mobile application user experience or even compromising cooperative gains in a cooperative scenario.

Protecting data from being disclosed, in its essence, boils down to the encryption process by making data unreadable for humans and/or machines. Furthermore, data exchange in such type of network must comprehend, among others, criteria like data confidentiality (data may be sensitive), data integrity (data may be altered during transmission), authentication (entities in communications have to prove their true entity), or non-repudiation (after a message being sent, the sender should not be able to deny it) [30].

Privacy's data protection for mobile health applications in a cooperative environment is the main topic of this dissertation and it will be carefully addressed along this document.

1.2. Problem Definition

In a typical m-Health system, information is exchanged between several entities, raising concerns about information privacy and protection. Such type of information may be considered as sensitive information and should not be made available to any other than authorized sources. Leak of information compromises patient's health data privacy and it may be used for secondary or improper use. Moreover, with the advent of mobile devices and, consequently, mobile health applications, the need to assure information privacy and protection is definitely a critical aspect for such applications. Cooperation mechanisms, as already stated, tend to be a current solution to guarantee overall connectivity, namely, in a mobile scenario. This approach raises few concerns regarding the information flowing among nodes through cooperation. Hence, the main problem approached in this dissertation refers to assure that all information flowing on the network through cooperation is protected from undisclosed sources, guarantying its privacy and protection.

1.3. Objectives

The main objective of this dissertation is the performance evaluation of available cryptographic mechanisms to present a consistent and robust solution for mobile health applications in cooperative environments. It essentially focuses on guarantying that health data from mobile applications is not compromised or disclosed to unauthorized or unwanted entities, while transmitted from mobile node to mobile node through cooperation. Hence, cryptographic mechanisms can be used to provide secure packet forwarding on the network, ensuring user health data confidentiality, integrity, and authenticity, i.e., it ensures data protection and privacy.

To accomplish this main objective, the following intermediate objectives were identified:

- A detailed study of the state-of-the-art in cryptography, approaches and its challenges, as well as the study of cooperation mechanisms for m-Health applications, along with the necessary review of mobile health and security issues related to e-Health;

- The system requirements analysis in order to fetch all the system requirements;

- Proposal and deployment of cryptographic solutions over cooperation mechanisms;

- Performance evaluation and validation of the proposed cryptographic mechanisms using a real prototype.

1.4. Main Contributions

This section is devoted to the scientific contributions of this dissertation to the state-of-the-art on mobile and ubiquitous health as well as on secure health data exchange through cryptographic mechanisms.

The first contribution presents a data encryption solution for mobile health applications (DE4MHA) with cooperation strategy for m-Health Applications. It aims to present a robust solution based on Encryption algorithms that guaranty the best confidentiality and protection of users health information. This contribution was published in the Journal of Medical Internet Research (JMIR) [31].

The second contribution of this dissertation is a performance evaluation of the cryptographic mechanisms for m-Health applications in a cooperative environment, including the proposal of a novel and enhanced cryptography solution in a cooperative environment called eC4MHA. This proposal aims to face the challenges related to privacy and security issues of all forwarded and retrieved data concerning user sensitive information in mobile health systems under a cooperative environment. A paper with this contribution was submitted to the IEEE Global Communications Conference (IEEE GLOBECOM 2013), Atlanta, USA, December 09-13, 2013. The paper is under review.

1.5. Dissertation Structure

This dissertation is organized in six chapters. This chapter, the first, starts with focus of the dissertation addressing the topic under study, identifies the research problem, defines the objectives, presents main contributions as well the dissertation structure itself.

Chapter 2 elaborates about the related work, approaching the literature on mobile health, including a brief review about ubiquitous health systems, focusing on the importance of ubiquity and usability. Then, cryptographic mechanisms are approached, along with some related work about health data exchange involving cryptographic solutions.

Chapter 3 approaches the requirements analysis for the cryptographic system presenting the essential requirements, UML diagrams (behavioural, interaction and structural diagrams), and the used technologies.

Chapter 4 addresses the considered cryptographic solutions. First, the cooperation mechanisms are shortly introduced along with the respective cryptographic measures that were applied. Next, the chapter focus on the cryptographic system architecture of the two proposed approaches.

Chapter 5 presents the performance evaluation and validation of the solutions. It presents a short presentation of the mobile health application used on the experiments, demonstrates the used network scenario, and focuses on the performance evaluation and validation of both considered solutions, which includes a comparison between them.

Finally, Chapter 6, summarizes all the work performed in this dissertation, considering the main conclusions of this work and suggestions for future work.

2. Related Work

In order to focus the scope of this dissertation, it is important to present some related work about the topic. Mobile health applications have been facing a considerable growth, much because of the also growth and acceptance of mobile technologies, namely smartphones and tablets. As an example, in the United States of America, 52% of smartphone owners have used their smartphones to look up for health info, whether through Internet researches or through usage of mobile health applications [32]. As mobile health applications evolve, more sophisticated and advanced health applications emerge, raising concerns about health data privacy and protection. Over the years, several attempts to standardize the way health data is exchanged between patients and doctors have appeared. In addition to the information structuration, that may enable easier and faster analysis by medical entities, it is also necessary to focus on assuring information privacy and security, once health information is in most cases sensitive information.

This chapter presents the related literature to mobile health in Section 2.1, approaching the different ways of structuring health information, in order to provide standard formats to transmit such type of data. In Section 2.2, security aspects are presented regarding e-Health, considering approaches that include privacy and protection of e-Health data. Section 2.3 briefly presents some cryptographic mechanisms, enumerating several efficient, and effective algorithms to perform operations related to cryptography. This chapter is summarized in the Section 2.4.

2.1. Mobile health (m-Health)

Over the years mobile health technology has been facing a tremendous development, given opportunities regarding patient’s health monitoring and treatment never seen before [33]. Although healthcare information systems are more suitable and designed for professionals to manage patients health records, mobile health has being offering to those who are isolated from healthcare facilities, new opportunities regarding their health status prevention and treatment. Elderly population is one of the most affected by isolation and displacement incapacities. Hence, mobile health is presented as an excellent solution for them. These people often underestimates diseases like hypertension and oversights that may cause several damage if not properly monitored for prevention and treatment awareness [34]. Through mobile health, data can be collected from patient’s mobile devices (e.g. smartphones or wearable sensors) and sent to healthcare providers, enabling a remote and fast analysis avoiding patient’s displacement.

Mobile technology has being registered a progressive evolution due to the growing ubiquity of those devices. Over the years, several definitions of ubiquitous computing have been proposed. One of the most widely cited definitions regarding ubiquitous computing [35] comes from Mark Weiser: “*The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it*”. In its essence, its goal is to provide users services available anytime and anywhere in a transparent manner, focusing in the information perceived by the user instead of the technology behind responsible for its operation [36], [37]. As it was already stated, mobile devices suffer from certain restrictions, namely their processing capacity, turning them inefficient to run heavy or poorly conceived algorithms with many processing tasks [38]. Hence, the development of ubiquitous Web-based systems has come to handle these limitations, releasing the mobile devices from running these heavy tasks, providing them access to remote services and content, regardless the time and place in a transparent manner. Ubiquitous computing may be present whether on client side (e.g. mobile device) or even in server side (e.g. Web Service). It offers invisible mechanisms, in a transparent way to the end-user. All the interactions with software and/or hardware happens without being noticed by the end-user [39]. As an example of a ubiquitous system used anywhere is the Internet itself, in which several services can be used in an invisible way. It helps users to maintain information (e.g. medical records), giving them the possibility to handle and access their information anywhere around the globe [37]. Ubiquitous health is also present in the use of body area networks (BANs) to make possible to ubiquitously monitor physical and physiological parameters [40]. In this type of system, also known as wireless body area networks (WBANs), data is collected through sensors, which is then ubiquitously sent and stored for later analysis by medical staff or even the patient itself. Data access may be accomplished through a neutral approach (e.g. a Web browser) [41]. A similar approach [42] deployed a long term healthcare system, in which a wireless local area network (WLAN) and a Cable Television (CATV) are used in a form of a ubiquitous network, allowing for patient physiological monitoring. Although ubiquitous systems present significant improvements, regarding health topic concerns, many ethical and privacy questions are raised as referred in [43]. Issues like knowing who owns the health information, who is allowed to access it, the way it is stored, and who is responsible for its management, are all matters that some users may have concerns about ubiquitous health care systems. In order to allow the natural grow of ubiquitous health systems and mobile applications, it is important to carefully study this issue and provide awareness to users of how data is being treated.

Due to devices ubiquity as well as due to mobile devices proliferation [44] several health applications have been developed and made world wide available to the public through online markets [45]. They offer to users the possibility of monitoring their own health state, by creating and maintaining their own health records, treatments alerts, health goals establishment, just to name a few. All these types of applications are present in many popular mobile platforms, such as Google Android OS [46], iOS [47], Symbian OS [48], and Windows Phone OS [49] with theirs respective applications stores, such as the Google Play [50] (formerly Google Android Market), App Store [51], Ovi Store [52] and Windows Phone Store [53], among others. Android OS is one of the preferred targets in what health applications concerns, with several applications available, like Stabilix PHR [54], that allows users to manage a personal health record. Another example is the Fast Food Calorie Counter [55] in which users can be aware of what they eat, or CardioTrainer [56] that makes use of GPS to keep track of the distance walked by the user, returning some performance information, as the calories burned in the walk. Regarding iOS concerns, Restaurant Nutrition [57] is an application that allows users to view nutritional information about restaurants menu and track what they have eaten. Capzule PHR [58] works as a personal health record for all the family, along with health in family [59] for Symbian. Lately, Windows Phone has been facing an increase of popularity among users, in which thousands of applications are being available everyday. Emergency Kit [60], it is an application that allows storing the blood type, allergies medications and emergency contacts. In case of an emergency, technicians will be able to view user’s health stats in a heartbeat. On the other hand, SapoFit [61] is a Google Android OS application that intends to be a more complete solution for obesity prevention and treatment. The use of Web services allows the system to be used anytime and anywhere. For integration and experiments of the cryptographic mechanisms, this application was used. However, more details about SapoFit will be properly addressed in Chapter 5.

Last approaches face several challenges, such as remote data collection, which may result in several problems regarding patient's health information structuration for efficient analysis as well as privacy and security issues. Poorly structured information may cause healthcare professionals to spent more time than required for data analysis as well as to misinterpret collected data, making the use of standards extremely important [62]. Furthermore, data retrieval from mobile applications is exposed to several threats while being collected or transmitted between several agents over the network. If all the necessary security requirements are not carefully addressed, e.g., assuring that all the collected data is kept confidential and their integrity untouchable, collected data may possible be compromised, eventually resulting in an improper or secondary use of such data.

Mobile health services are present in a large scale in the applications available to users, allowing them to obtain useful information about their health care, serving as well as prevention awareness. Furthermore, mobile health is commonly used in telemedicine allowing, such as, personal health care, remote management, and patient's health status monitoring [63]. A proper structuration of such information along with its security and privacy becomes an essential point. In [64], some challenges and limitations on m-Health systems are presented, namely the lack of standards regarding the standardization to link telemedicine services, due to difficult operational compatibilities between mobile devices and telecommunications services. Moreover, it is stated that due to system privacy and security issues, user acceptance tends to grow up slowly.

Electronic health records (EHRs) and health level seven international (HL7) protocols can be considered as a solution, allowing efficient information structuration, enabling easier interpretation of such information by different entities.

2.1.1. Electronic Health Records

A common way for healthcare providers to usually store health information is electronic health records (EHRs) [65]. An EHR is essentially a representation of health information in an electronic format [66]. It enables faster and more convenient access by physicians or medical staff. A typical EHR system is based on a well structured and organized archive regarding the patient medical history in an electronic form [67]. An EHR presents several advantages regarding health information structuration, namely the capacity to improve health providers efficiency, reducing costs or even increasing treatments effectiveness [68]. Moreover, it allows medical staff or patients to easily access that information in an electronic way providing to the medical staff enhanced abilities to make improved decisions about possible health treatments or analysis to the patients health information [69]. An illustration of a typical EHR mobile system architecture [70] may be seen in Figure 3.

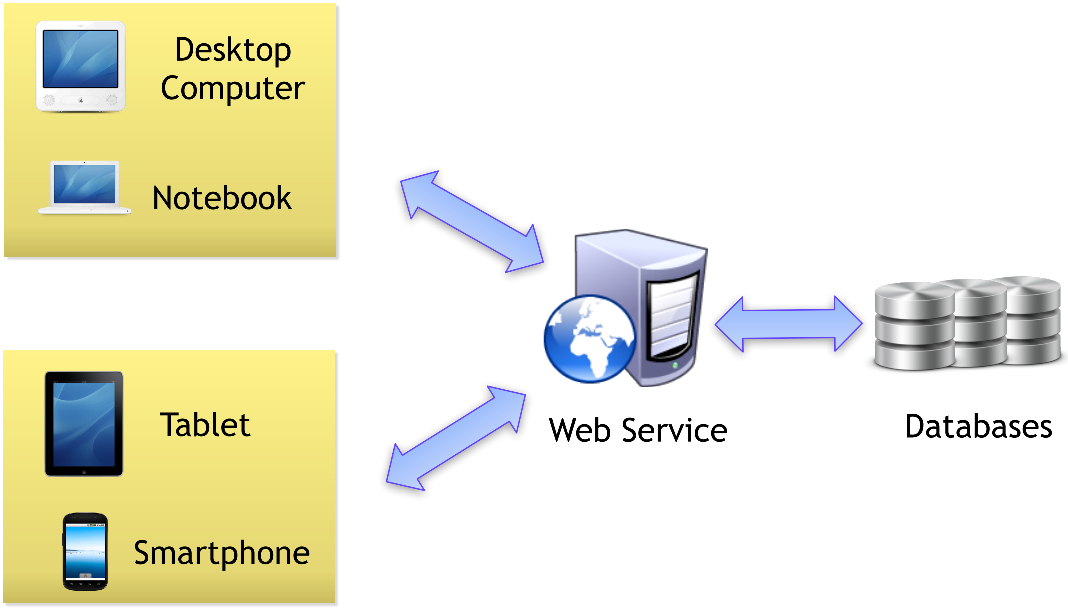


Figure 3 - Illustration of a typical EHR mobile system architecture.

EHR-based mobile applications are currently gaining popularity due to the fact that users access their health information through the Web, not being constrained to spatial and temporal barriers, although it is necessary a reliable Internet connection in order to support these services [71]. Mobile-EHR (m-EHR) systems rely on the utilization of Web Services that enable the access to data from any personal computer, tablet, or smartphone with Internet connection [72].

Current limitations regarding EHR adoptions among patients, include the above-mentioned issues related to information privacy and potential security concerns [73], mainly due to the fact that EHR may hold sensitive information. Another drawback in the utilization of EHR systems regards interoperability. Achieving interoperability between systems using EHR systems managed by different healthcare providers still presents slowly and expensive tasks [74]. In this sense, HL7 is presented as a standard with main goal directed to achieving interoperability among systems with different healthcare providers.

2.1.2. Health Level Seven International (HL7)

Health level seven international (HL7) is a non-profit, ANSI-accredited standards developing organization, that intends to deliver and provide a framework and related standards for the exchange, integration, and retrieval of electronic health information [75]. HL7 was created in 1987 in the United States of America. In its essence, HL7 protocol is a set of protocols specifying how electronic health data should be exchanged in healthcare environments, between computer applications that may belong to different manufacturers. Information sent through HL7 standards is sent as a collection of one or more messages, in which each one of them carries health information (records), e.g., patient records or laboratory records. Over the years, its strategy has been refined, as may be seen in the different versions that have come out, as illustrated on Figure 4. The currently version is the HL7 version 3, which is based on the reference information model (RIM) [76]. It basically allows specifying the information content of messages, through an information model that clarifies definitions ensuring that they are used consistently. While HL7 v2 provides a negotiated framework for developers to easily use and adapt, v3 was targeted for being a stricter standard that aimed to eliminate variances, in an effort to improve interoperability between all users of the standard [77].

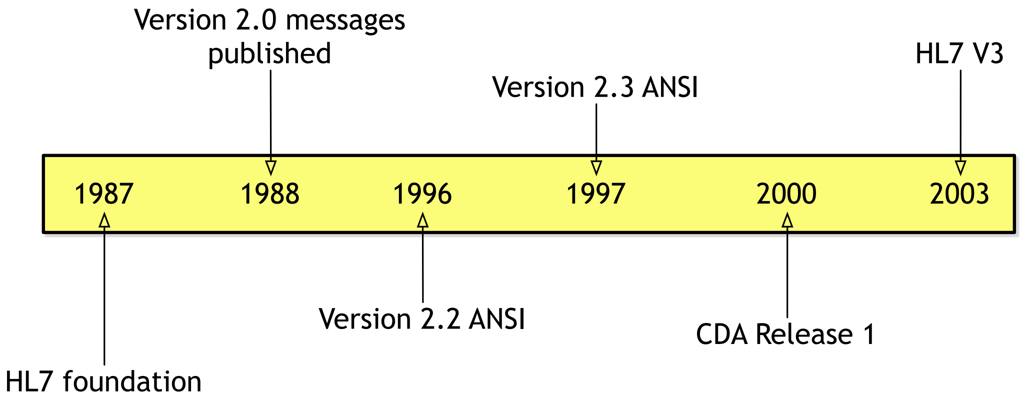


Figure 4 - HL7 history.

HL7 v3 is based on messages and aims to be easily interpreted and processed by machines. On the other hand, HL7 has developed the clinical document architecture (CDA), that is a generic message structure to be able to exchange clinical documents, based on the HL7 RIM, but unlike the HL7 v3 protocol, its main goal is to assure effective and better human readability, although it was developed for being easily interpreted and processed by machines as well. The CDA is structured in eXtensible markup language (XML) and it specifies the semantic structure of how a clinical document, with exchange purposes, should be codified. It is the base model of any clinical document that may be exchanged between different entities.

HL7 has been offering a standardized way of exchanging e-Health data among machines or devices that deploy and follow the HL7 protocol. Through a protocol like HL7, different machines from different vendors can communicate through a standard interface, allowing to add new machines without modifying the original source system, as may be seen in Figure 5.

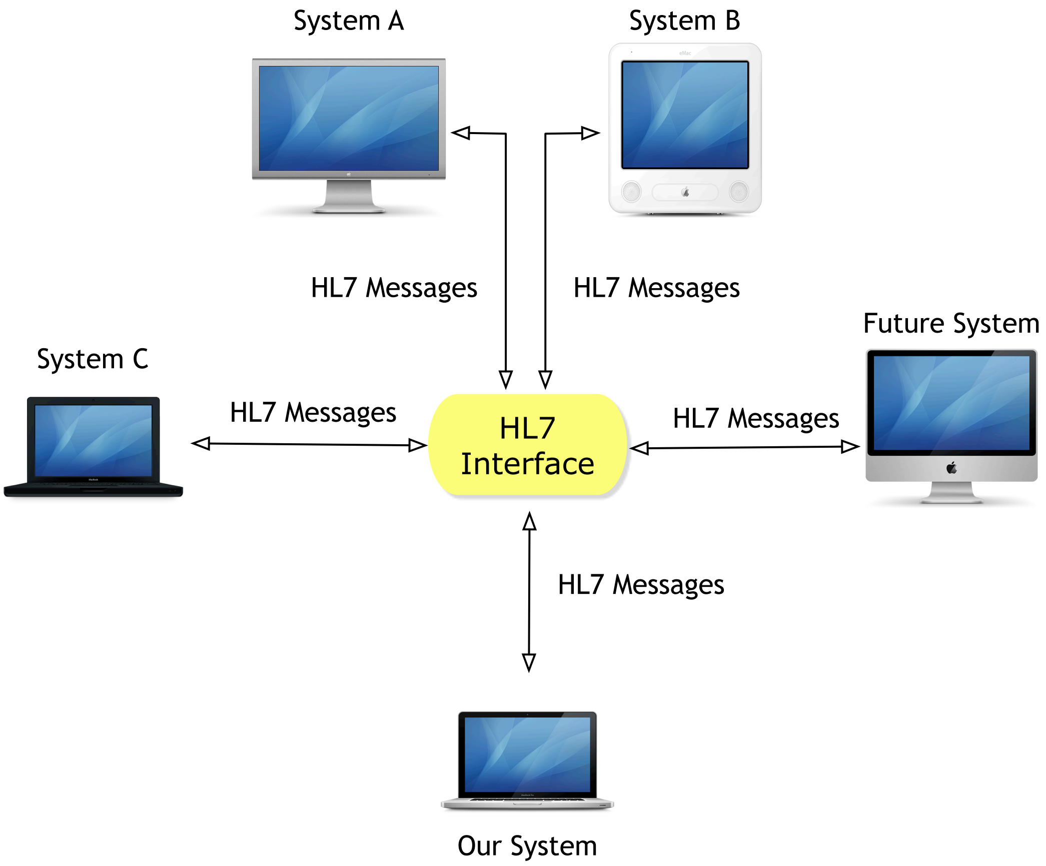


Figure 5 - Illustration of an HL7 Interface model.

Although HL7 protocols specify conveniently how data should be properly structured, several security issues arise. Through HL7 protocols health information is carried and, as above-mentioned, such information may be sensitive. Fortunately, HL7 organization offers guides to identify and solve potential security issues. One of the recommendations of HL7 is to use the secure socket layer (SSL) to encrypt communications between applications. SSL is a security standard that allows establishing an encrypted link between a given server and a client, usually a Web server (Website) and a browser. It uses asymmetric cryptography for key exchange authentication, symmetric encryption for confidentiality, and message authentication codes for message integrity (Cryptography will be more detailed in section 2.3). This approach prevents data disclosure when attempts to sniff HL7 network traffic occur. Furthermore, HL7 organization has been creating its own standards regarding privacy and security, like the role based access control (RBAC) method that essentially controls access to resources on an information system, or the CDA consent directive, that defines privacy policies on how individually identifiable health information (IIHI) should be collected, accessed, used, and disclosed. Although those standards should come to offer a uniformed and unique way of exchanging information, with a standard structure following privacy and security standards, its employment requires a long and slow period of time in order to be able to perfectly understand and apply such standards.

Lately and largely due to the advent of mobile health technology, HL7 decided the creation of a working group, focusing on developing and promoting standards for e-Health data exchange towards mobile health technology. It follows the same principles as the previous standards, i.e., it focuses on interoperability. Unfortunately, this working group is still in an early phase of development, as there are yet no available standards for commercial use. Originally, HL7 standards were intended to be used in the context of this dissertation but the lack of available standards for mobile technology motivated other approaches for this study.

2.2. e-Health data privacy and protection

Over the years, concerns about securing e-Health data has been a matter with great importance, mainly due to the sensitivity of data exchanged between users [78]. Since m-Health applications may carry sensitive health data about patients (e.g., infectious diseases such as HIV), it clearly becomes extremely important to give the appropriated attention to all of these issues when developing m-Health applications, in order to ensure that user's health data privacy is not compromised. One of the most common solutions to handle security issues in such cases is cryptography [79]. In [80], it is proposed an architecture that allows exchanging patients' medical record in a secure way through the existing infrastructure of mobile operators. Generic bootstrapping architecture (GBA) is used to enable user authentication, while the other entity in the communication (service provider, hospital, and network operator) authenticates through usage of public key infrastructure (PKI). To guarantee a secure communication, encryption, and digital signature techniques are used.

In [81], it is presented an approach to protect data considering a scenario composed by a user with wearable sensors with the possibility of transmitting collected data not only from the sensors to a mobile phone (through Bluetooth), enabling vital signs monitoring and analysis, but also from the mobile phone to trusted medical professionals. In order to assure confidentiality of the data transmitted between a mobile phone to trusted devices, authors do not rely on the security provided by Bluetooth and WLAN technologies, applying instead the AES algorithm with a key size of 128 bits, in combination with message authentication codes. For data transmission in a secure way, it is necessary to establish a mutual authentication between the user's mobile phone and the trusted devices, which is achieved using the Diffie-Hellman key exchange protocol for session key agreement, assuring this way a safe session key transfer.

In [82], authors describe a new trend in security of e-Health data, presenting XML security solutions, describing some selected solutions in health data. eXtensible access control markup language (XACML) and security assertion markup language (SAML) are presented, enabling authentication and authorization in a large network space. SAML enables transmission of authentication data between parties, namely between an identity provider and a service provider. XACML defines access control policies and a processing model, describing how to evaluate authorization requests according to the rules defined in the policies.

Another approach regarding secure e-Health data retrieval and transmission is proposed in [83], within a context where mobile phones can be used from anywhere to access health information stored in remote databases. To secure transmitted information from/to the remote databases, a policy regarding who may access such information is employed using authentication and access control. Authentication is based upon the types of users authorized to use the m-Health application, by providing a secured username and password. To provide the necessary security on transmitted data, an elliptic curve cryptography algorithm is used, encrypting data retrieved from the database, which is then sent to the mobile phone through wireless and decrypting it on the mobile application.

The above-mentioned approaches present features required in an m-Health scenario, essentially covering scenarios where an m-Health application running on a mobile device, retrieves or transmits information from/to remote databases, using service oriented architectures (SOAs). All the above-mentioned approaches essentially focus on the use of cryptographic mechanisms, by primarily using techniques of encryption to assure data confidentiality. To guarantee that retrieved and collected data it is not modified, an awareness of such modifications should be provided, which is also considered in last approaches by using signature techniques. However, some limitations arise, specifically the first one suffers from mobile operator dependency, while the third one is focused towards systems exchanging data in XML format. Furthermore, cooperative scenarios present their own specific features and limitations, such as node misbehaviour, connections loss, or even different formats of data exchange, requiring special care. Thus, a comprehensive study of cooperation mechanisms becomes an important step towards the development and application of effective and efficient cryptographic mechanisms. Next section provides an awareness of cryptography to better understand in what exactly consists, as well the several existing algorithms with better performances available.

2.3. An Overview of Cryptographic Approaches

Cryptographic mechanisms have proven to be a promising solution for several security issues in wireless networks, as may be stated in the above-given examples. In this sense, cryptography may be defined as a set of techniques that tries to assure safe communication between two agents, on an open channel. It essentially tries to give an answer to numerous proprieties of the communication process like confidentiality, integrity and authenticity [84]. This section will focus on briefly describing the above-mentioned properties. It will also enumerate several cryptographic algorithms, used world wide, to secure the most diverse kinds of data.

2.3.1. Confidentiality

Confidentiality consists in protecting data within a message from being available or disclosed to unauthorized persons [85]. Therefore, referring confidentiality, it implies dealing with encryption. Encryption can be defined as the process of encoding messages in a manner that no one else but authorized parties should be able to read. On the other hand, it exists the decryption procedure, which is the inverse process of encryption, i.e., it consists in decoding the encrypted message, in order to obtain its original content. Hence, several algorithms were developed and presented over the past decades to deal with the increasing need of assuring data confidentiality, and they may be split into two main groups, *i*) symmetric algorithms where both encryption and decryption is accomplished using the same key, and *ii*) asymmetric algorithms, where one key is used to encrypt (public key) and another one is used in the decryption process (private key).

2.3.1.1. Symmetric Algorithms

Several well-known symmetric key encryption algorithms and enumerated in [86] have been examined, namely: data encryption standard (DES), triple data encryption standard (3DES), advanced encryption standard (AES), blowfish, international data encryption algorithm (IDEA) and Rivest cipher 4 (RC4). To present an overview of how these types of algorithms operate, DES algorithm can be used as example. It operates on a 64 bits data block and a fixed key length of 56 bits size for 16 rounds, i.e., it splits the original data in fixed blocks of 56 bits applying then 16 rounds of the required operations to produce a cryptogram, as may be seen in Figure 6.

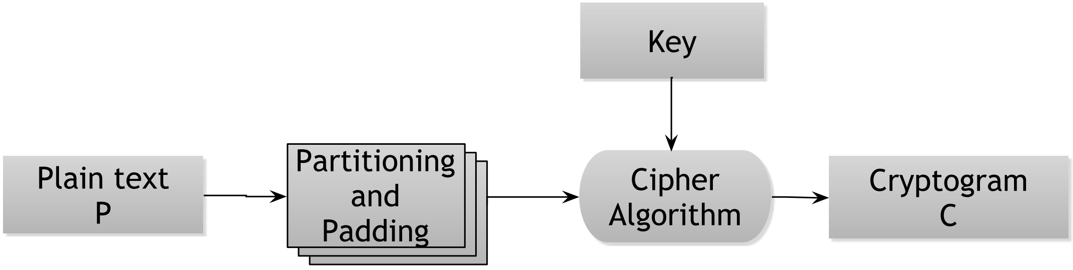


Figure 6 - General symmetric algorithms processing sequence.

Nowadays, it is considered out-dated and it has been replaced by its successor 3DES, that essentially consists in applying DES algorithm three times rather than one, supporting 112 bits or 168 bits key of length, and a block size of 64 bits, that operates on 48 rounds and it is, therefore, considered to be inefficient. On the other hand, AES algorithm operates on a block cipher of 128 bits size and the key size is 128, 192 or 256 bits [87]. AES is a 10,12 or 16 rounds iterative cipher that uses byte substitution, row shifting, column mixing and key addition presenting a fast encryption/decryption speed due to being based on the shifting operations.

RC4 also known as ARC4 or ARCFOUR, was designed by Ron Rivest in 1987 and uses a variable key length, i.e. from 40 to 256 bits, as well variable block size, what makes its speed in encryption/decryption varies. Secure socket layer (SSL) handshake protocol uses RC4 to encrypt/decrypt traffic to and from Web Sites. Finally, IDEA it is best known for its use in pretty good privacy (PGP) v2.0. It is an algorithm that operates on a 64 bits block size with a 128 bits key size.

2.3.1.2. Asymmetric Algorithms

These type of algorithms, also known as public key cryptography, solve some of the faults of the symmetric algorithms, such as the obligation of using the same key between two parties to encrypt/decrypt, although they are considered to be at least one thousand times slower than symmetric ones [88]. Keys size have to be significantly bigger (e.g. a 1024 bits key of an asymmetric algorithm, corresponds approximately to a 128 bits key of a symmetric algorithm) and it is usually harder to handle key management [89]. These types of algorithms are normally used with identification purposes or to session key exchange, without requiring a trust agent. RSA [90] is an example of an asymmetric algorithm and its name stands for Rivest, Shamir and Adleman, the founders of the referred algorithm. It is widely known by being appropriated to encrypt/decrypt as well to perform digital signature. It was proposed in the late 70's but it is still used nowadays. Another example of asymmetric algorithm is Elgamal [91] widely known as alternative to RSA and it is considered to be simple and efficient.

2.3.2. Integrity

Integrity aims to provide an awareness of the correctness and consistency from a specific stored or transmitted data, Indicated by the absence of any change in such data after update or transmission [92]. As an example, health information is known as sensitive information in which a small change of the original information may have a negative outcome. Therefore it is usually a good idea to use algorithms that can assure us that we're handling unchanged and original information. Hence, cryptographic hash functions are used for that purpose. Message digest 5 (MD5) [93] designed by Ron Rivest is a largely used hash algorithm to check data integrity. It produces a 128 bits output called message digest. To check data integrity, the same fragment of data, must always produce the same message digest as output, though in rare cases it may produce the same message digest for different fragments of data [94]. Secure hash algorithm 1 (SHA-1) [95] is another algorithm which main purpose it is to assure data integrity, producing a 160 bits message digest. Both algorithms allow checking data integrity, by computing the message digest of a certain message. Any change of the message, will almost certainly result in a different message digest, which allows checking if data integrity has been compromised or not.

2.3.3. Authenticity

Authenticity is another important concept when handling with security mechanisms. Nowadays, in every system, it is vital to assure that we're communicating or receiving information from the expected source. Therefore authenticity can be achieved using an asymmetric algorithm like the above-mentioned RSA algorithm, in combination with a hash function, in which the private key is used to encrypt the message digest produced by MD5 hash algorithm. Then, the public key is used to decrypt the message digest, and when compared with the generated message digest on the sender's side, both must be equal, as illustrated in Figure 7.

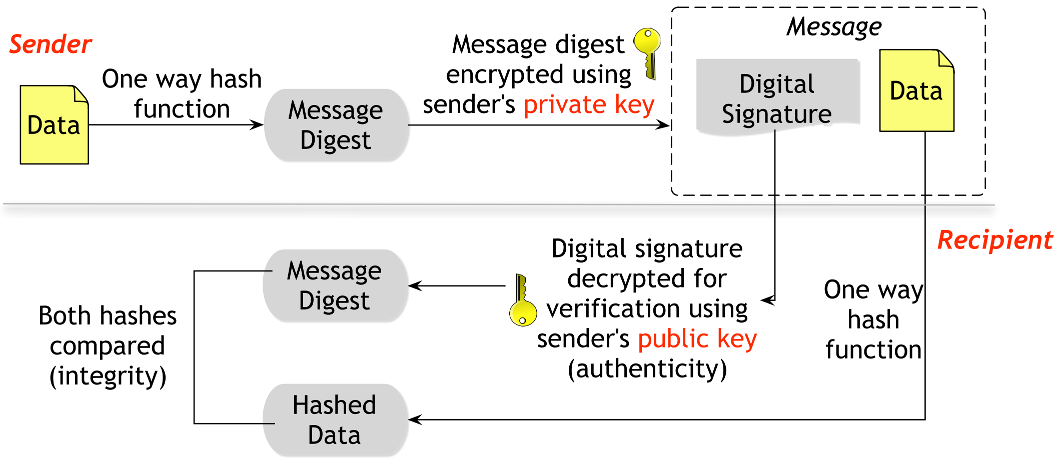

Sender
Data
One way hash function
Message Digest
Message digest encrypted using sender's private key
Message
Digital Signature
Data
Recipient
One way hash function
Digital signature decrypted for verification using sender's public key (authenticity)
Message Digest
Hashed Data
Both hashes compared (integrity)

Figure 7 - Digital Signature.

Digital signature algorithm (DSA) [96] also provides digital signature capabilities. However DSA can only sign not providing encryption capabilities, furthermore it uses SHA-1 to generate the message digest as opposed to MD5 algorithm used by RSA. David Kravitz developed DSA and National Institute of Standards and Technology (NIST) adopted it as a Standard in 1991.

The previous presented properties are usually the main features that should be addressed when attempting to provide security to some given data, whether or not a mobile environment is considered. The work presented in this dissertation focuses on the previous cryptographic approaches, by applying them to mobile health data in a cooperative environment, as it will be approached in the next chapters.

2.4. Summary

This chapter presented the literature review concerning mobile health, ubiquitous health and cryptographic mechanisms. Thus, after a brief introduction, Section 2.1 presented the mobile health review along with a review on ubiquitous health regarding monitoring systems as well as mobile devices applications for common users. Section 2.2 presented some related work regarding e-Health data transmission between different entities focusing on data privacy and protection issues. Section 2.3 briefly presented some of the cryptographic mechanisms available, presenting algorithms used in cryptography.

3.Requirement Analysis

Software development must always contain all specifications of the system to create. Therefore, requirement analysis, also called requirement engineering, is an essential part and its existence is mandatory to fully identify all system features and behaviours.

The most used modelling specification is Unified Modelling Language (UML) managed by the Object Management Group (OMG). It provides suitable standard methods to model applications and data structure as well its behaviour, architecture and business process [97]. Although UML is not a software methodology or a programming language, it is a language with semantic notation that allows developers to view, specify, build and document the objects of a system that makes possible to design models, which consists in a set of a diagram with textual description that are consistent with each other.

The system features and behaviours will be addressed in this chapter along with UML diagrams in order to demonstrate behaviours, interactions and the system architecture.

Section 3.1 will approach the system essential requirements, Sections 3.2 to 3.4 will present behavioural, interaction and structural diagrams for both approaches (DE4MHA and eC4MHA) and Section 3.5 will address used technologies. In Section 3.5 is shortly presented the Android architecture. Last, Section 3.6 summarizes the chapter.

3.1. Essential Requirements

One of the most relevant steps in requirement analysis is to determine essential requirements. They can be features or constraints, where the requirements that are mandatory to be present in the future system are established. Defining essential requirements can be a difficult task due to the need of having a global and complete vision of the future system to fully define these requirements. Hence, the following essential requirements were defined:

- Android API level should be equal or above 10 (i.e., Google Version equal or above 2.3.3), which represents 94,2% of the active Android devices across the globe [98];
- Bluetooth hardware should be present;
- Wi-Fi or Edge/3.5G/4G modules are required;
- Cooperation mechanisms should work ubiquitously in the system;
- A pervasive Web Service is required in order to provide access and data management;
- Cryptographic mechanisms should works ubiquitously in the system and thus, completely invisible and transparent to the end user;

In order to create and integrate the mobile cryptographic mechanisms, the above-defined essential requirements are required.

3.2. Behavioural Diagrams

Behavioural diagrams are used to represent system functionalities, i.e., it shows what must occur in the modelled system and it comprises use case and activity diagrams.

3.2.1. Use Case Diagrams

Use case diagrams can be used to describe global system functionalities, by describing a set of actions (use cases) that the system (subject) should or can perform with one or more external user to the system (actor). The general use case diagram for the m-Health application is presented at Figure 8.

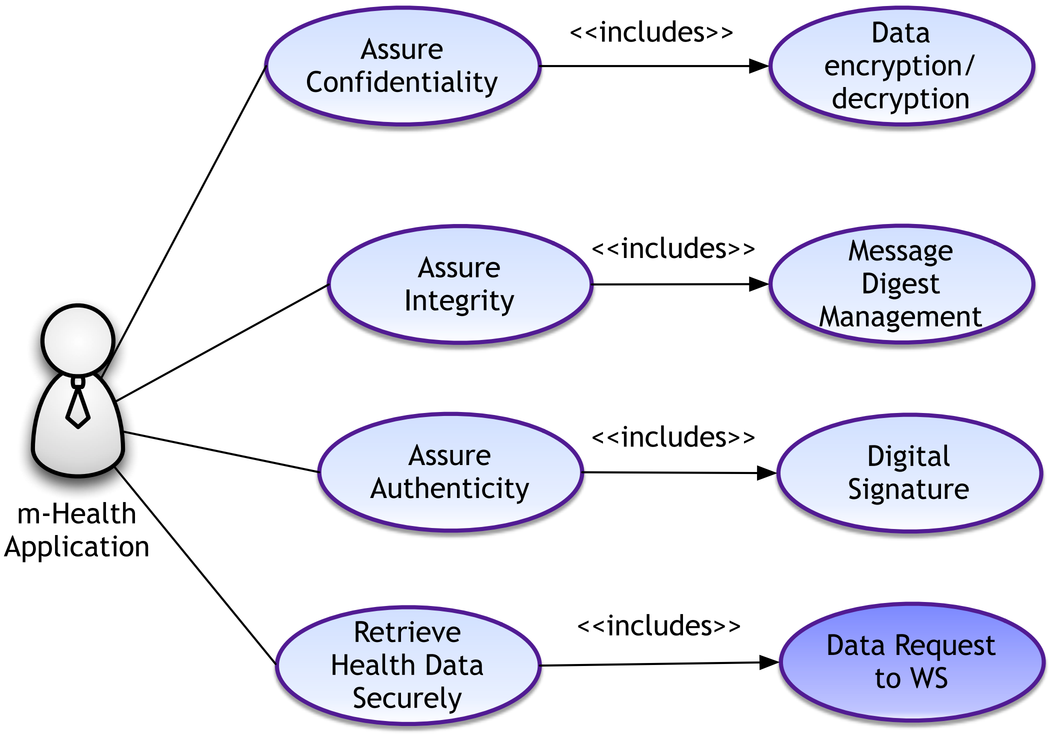


Figure 8 - Application use case diagram.

3.2.2. Activity Diagrams

Activity diagrams are widely used to provide a visualization of the system workflow. Two activity diagrams are defined regarding DE4MHA and eC4MHA approaches. In Figure 9, it is presented the activity diagram of

DE4MHA, that shows the secure health data retrieval workflow between mobile devices and the WS, when a node makes a service request.

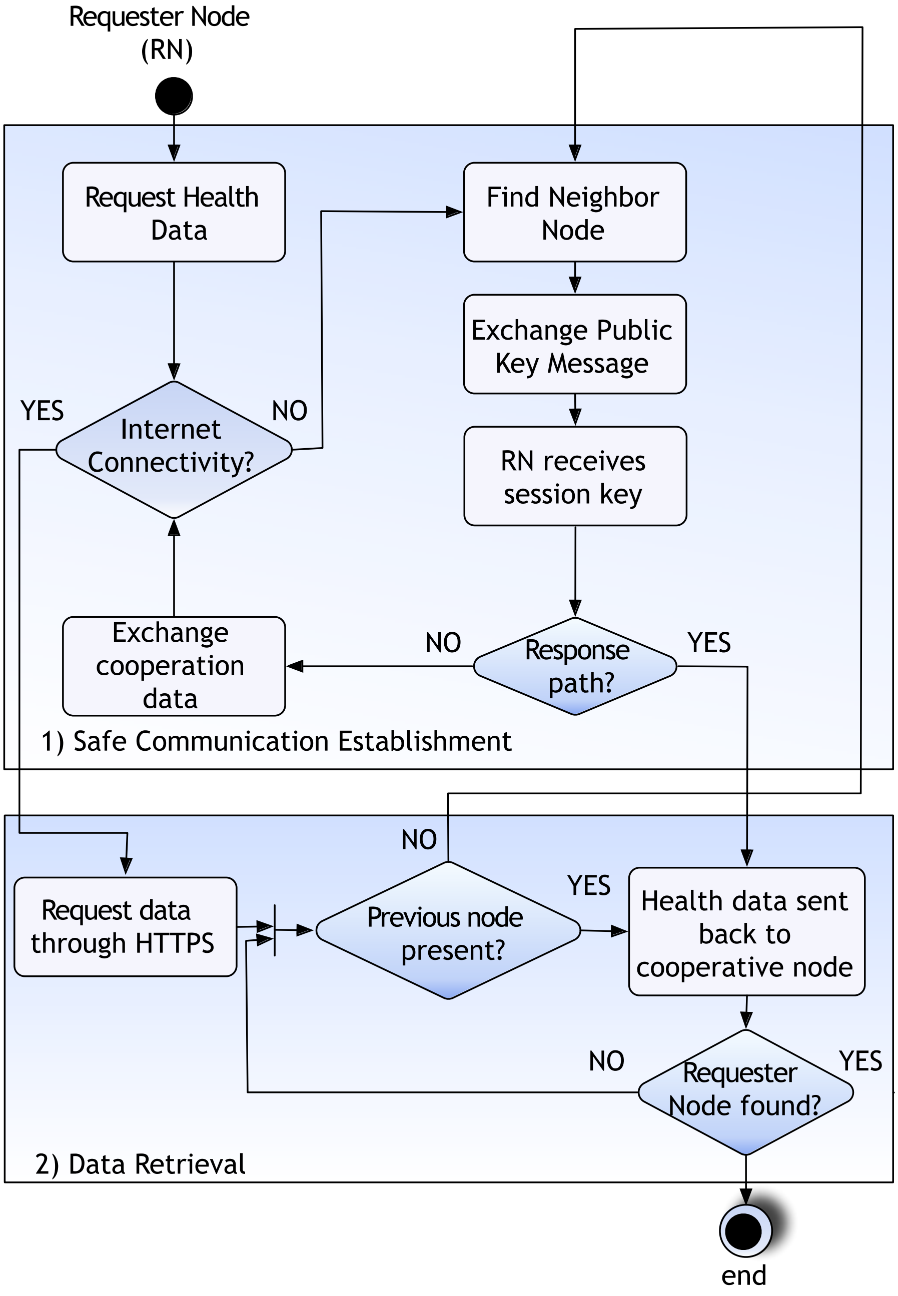


Figure 9 - DE4MHA activity diagram.

In the following Figure 10 is presented the activity diagram regarding eC4MHA workflow.

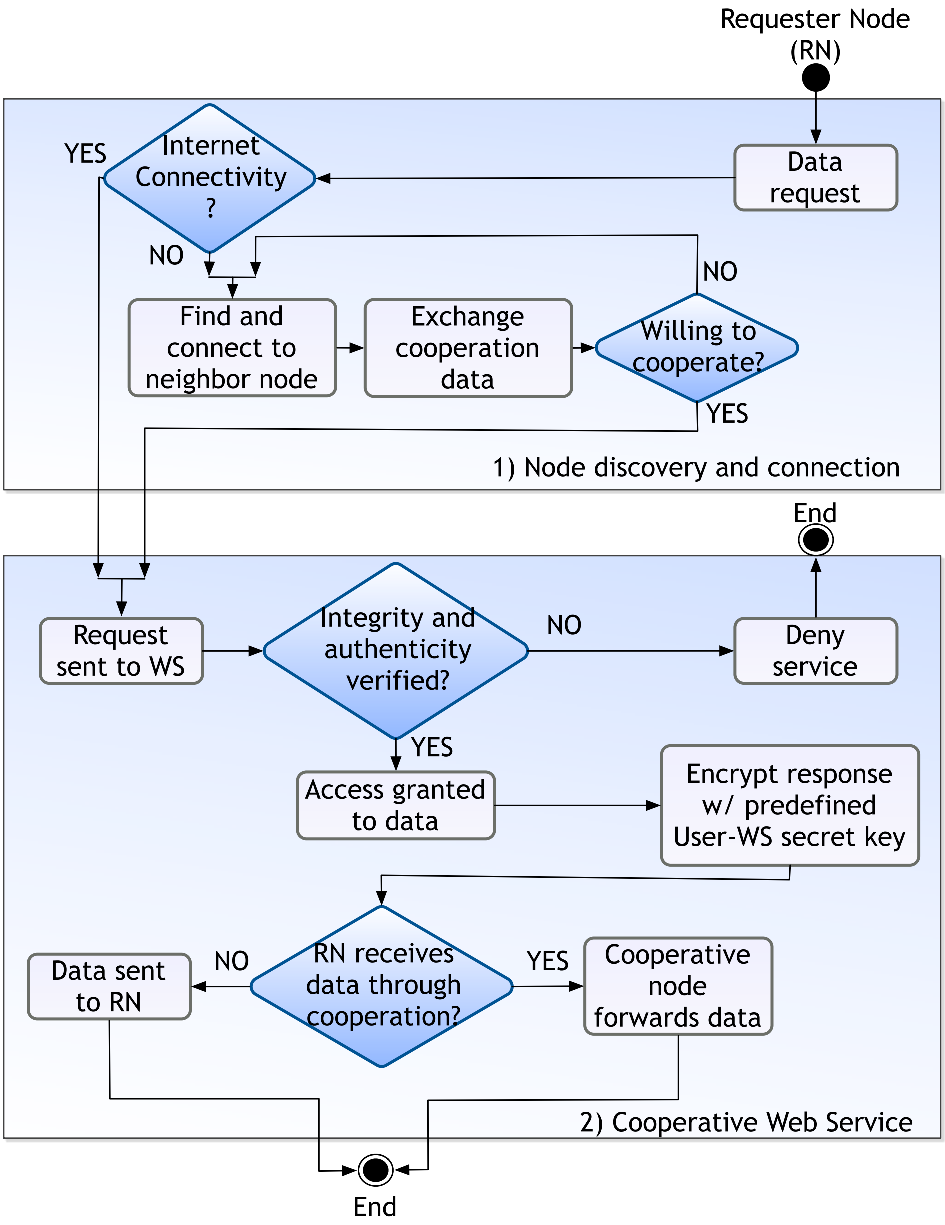

Requester Node
(RN)
Data request
Internet Connectivity ?
YES
NO
Find and connect to neighbor node
Exchange cooperation data
Willing to cooperate?
NO
YES
1) Node discovery and connection
End
Request sent to WS
Integrity and authenticity verified?
NO
Deny service
YES
Access granted to data
Encrypt response w/ predefined User-WS secret key
RN receives data through cooperation?
NO
YES
Data sent to RN
Cooperative node forwards data
2) Cooperative Web Service
End

Figure 10 - eC4MHA activity diagram.

3.3. Interaction Diagrams

Interaction diagrams are used to describe interactions among elements in the system.

3.3.1. Sequence Diagrams

Sequence diagrams are useful to model the logic flow within a system perspective. They focus on identifying the system behaviour. In this work the system flow was divided in two relevant diagrams. The first one illustrated at Figure 11, presents the DE4MHA sequence diagram.

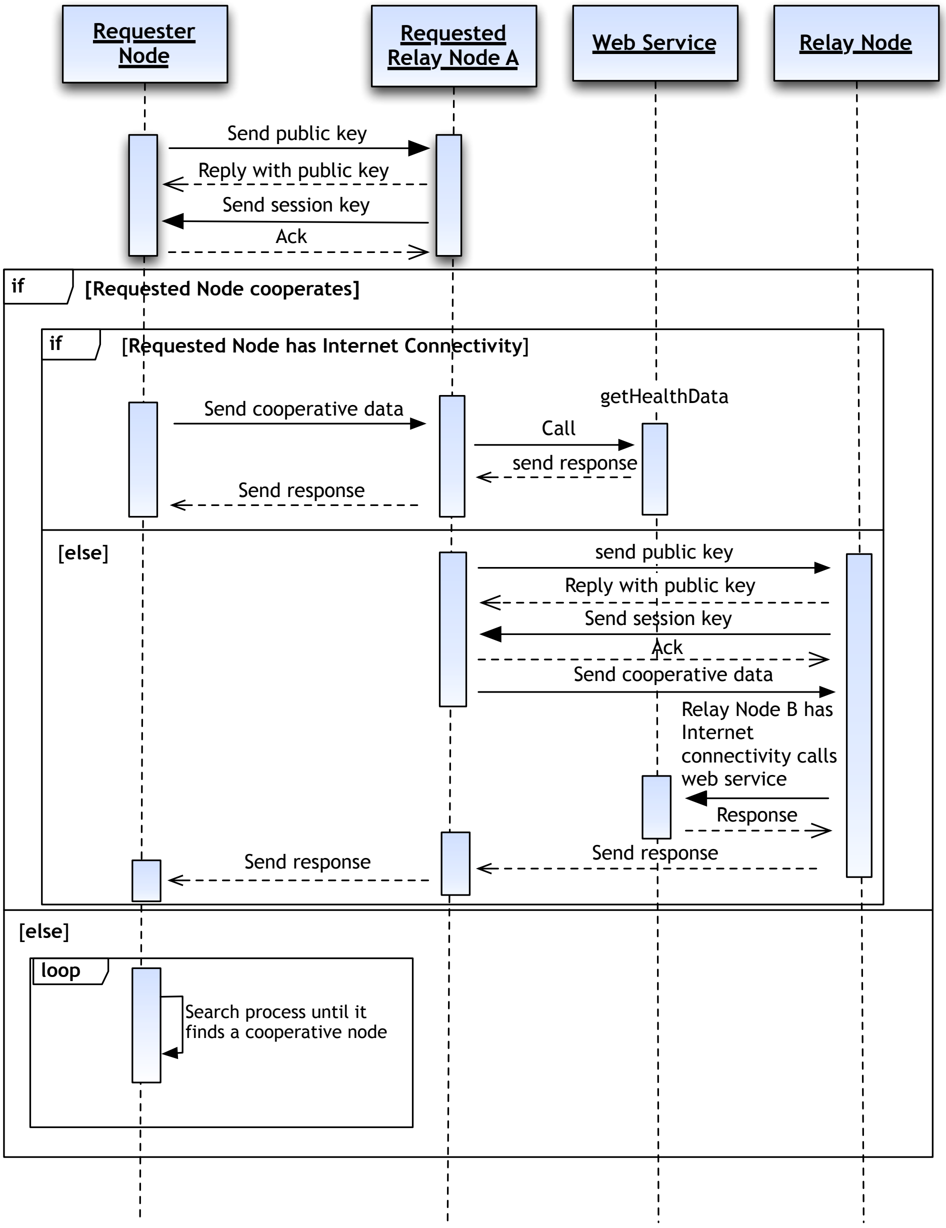


Figure 11 - DE4MHA sequence diagram.

The next sequence diagram, presented in Figure 12, represents eC4MHA connection to WS for session key retrieval as well to health data retrieval, whether cooperation is required or not.

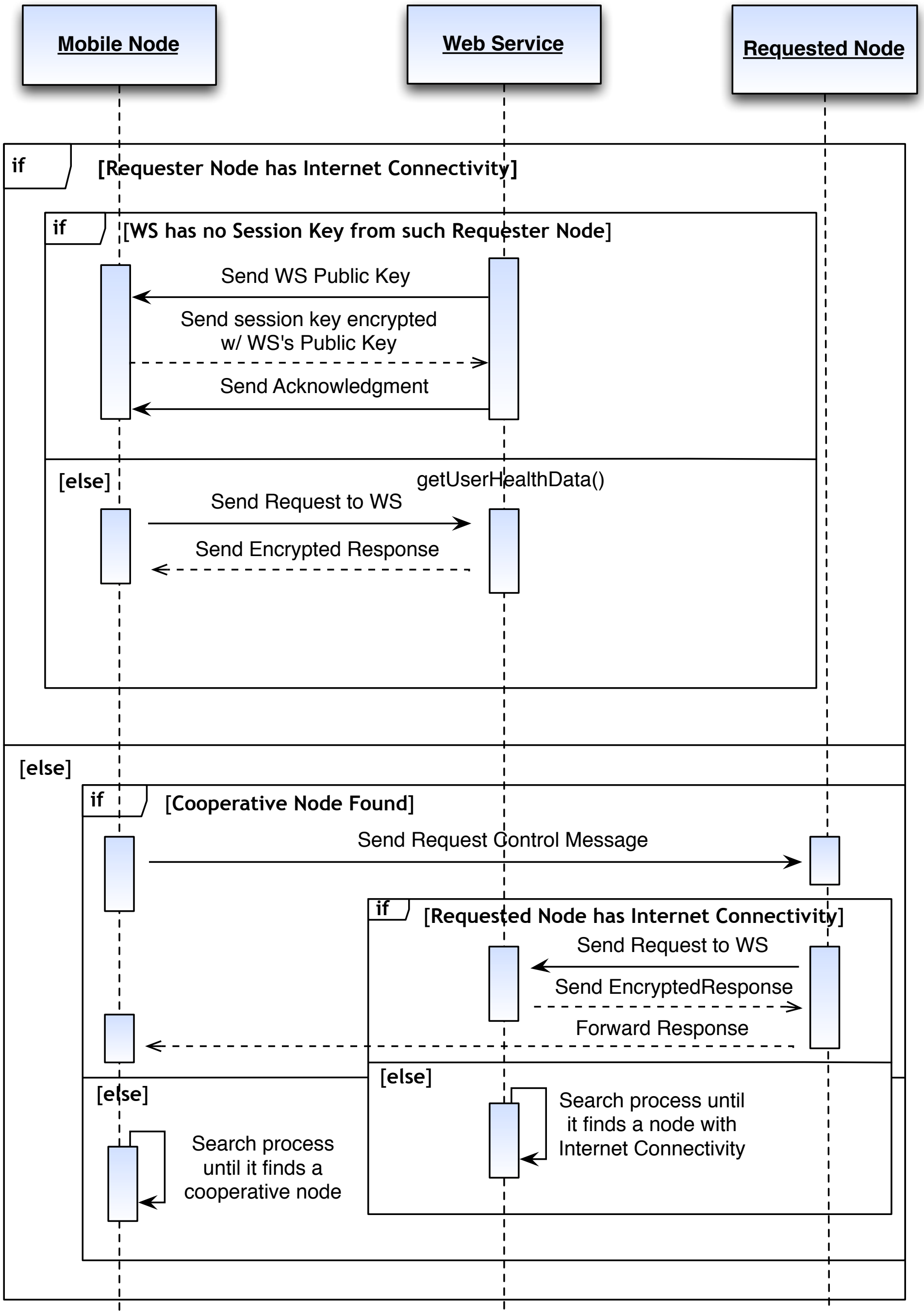

Mobile Node
Web Service
Requested Node
if
[Requester Node has Internet Connectivity]
if
[WS has no Session Key from such Requester Node]
Send WS Public Key
Send session key encrypted w/ WS's Public Key
Send Acknowledgment
[else]
getUserHealthData()
Send Request to WS
Send Encrypted Response
[else]
if
[Cooperative Node Found]
Send Request Control Message
if
[Requested Node has Internet Connectivity]
Send Request to WS
Send EncryptedResponse
Forward Response
[else]
Search process until it finds a node with Internet Connectivity
[else]
Search process until it finds a cooperative node

Figure 12 - eC4MHA sequence diagram.

3.4. Used Technologies

The proposed cryptographic solutions aim mobile devices running Google Android operating system, shortly described in the next section. However, the proposed strategies could also be applied to other mobile operating systems, such as iOS or Windows Phone. Hence and in order to be possible to apply such mechanisms, Android Software Development Kit (SDK) [99] was used, which provides the necessary tools and a set of APIs to develop android applications using the Java programming language. More specifically, *javax.crypto* package was used to deal with the low levels of cryptography, enabling encryption, decryption and hashing operations. To manage the other aspects regarding cryptography, it was used the *java.security* package, which enables, among others, to handle key management and digital signature operations. Both packages are part of the Java cryptography architecture (JCA) or Java cryptography extension (JSE).

The development tool used to develop the different proposed approaches with cryptographic mechanisms, was the Eclipse integration development environment (IDE) in combination with the Android development tools (ADT) plugin, designed to extend Eclipse capabilities, providing debugging options or even test emulators.

The required modifications to the existing Cooperative Web Service (CWS) were accomplished with the original technology employed in the cooperation mechanisms, namely the Java Server Pages (JSP) technology [100], using the REST architecture.

3.5. Android Platform

Google Android is a software stack for mobile devices that includes an operating system, middleware and key applications. The Android SDK provides the necessary and required tools and APIs to be able to develop applications for the Android platform, using the Java programming language. The following Figure 13 shows the main system components of the Android OS.

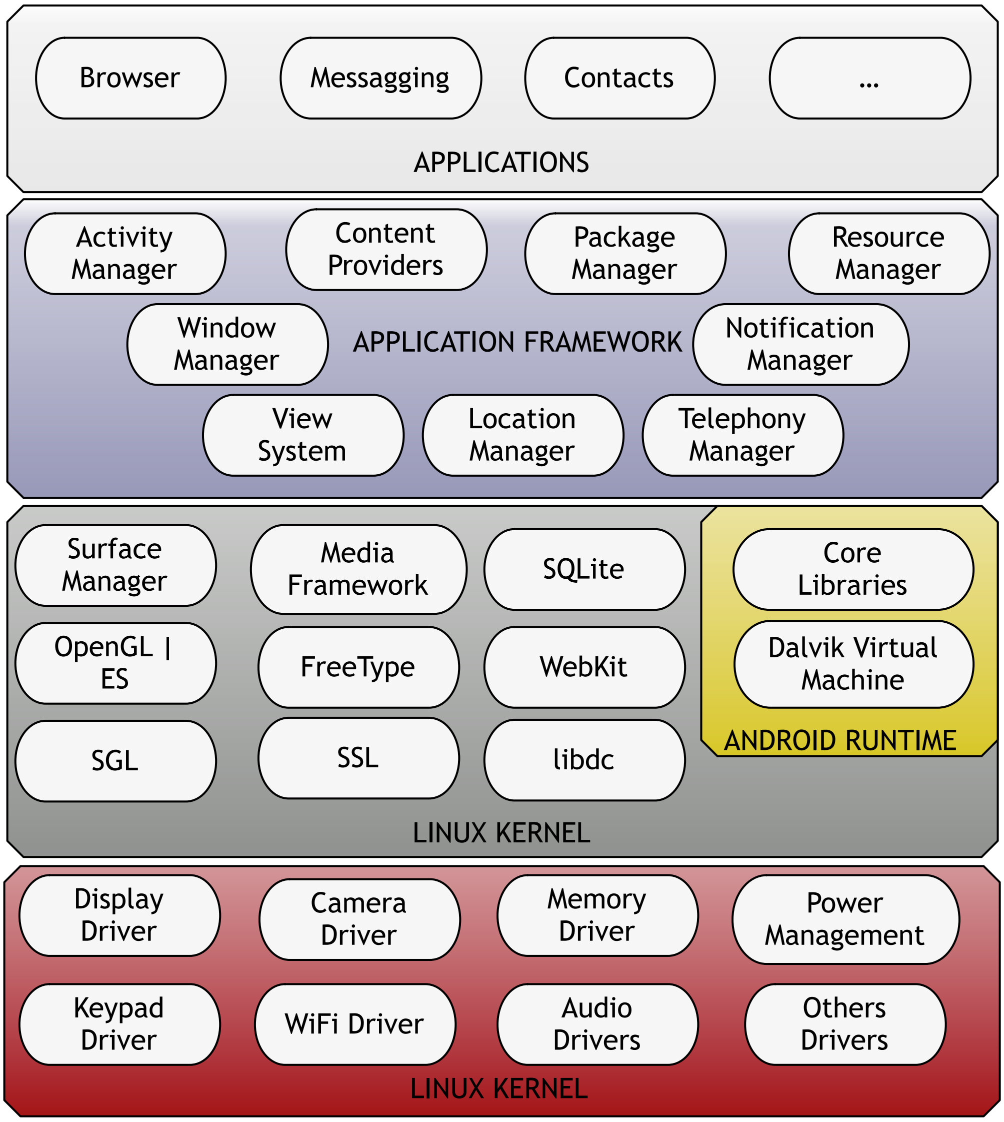


Figure 13 - Android OS architecture.

The above shown components may be summarized as follows:

- **Applications**: Android OS provides by default a set of core applications, such as email client, phone dialler, messaging app, calendar, maps, browser, among other applications;

- **Application Framework**: Through this framework it is possible to access device hardware management options, as well access to the location information and other embedded android features;

- **Libraries and Android Runtime**: A set of libraries used by several components of the OS and explored by the application framework as well the Android Runtime, that comprises core libraries and the Dalvik Virtual Machine (DVM) are included in the Android OS;

- **Linux Kernel**: The kernel handles core system services such as memory and process management, working as an abstract layer between the hardware and the software stack.

Android possesses an activity stack that manages the different activities that an application may have. Given that an activity may be unexpectedly terminated, whether by the system or by the user, poses problems in the normal application functioning. Therefore having a reasonable knowledge of the Android architecture becomes mandatory in order to be possible to design and develop robust and consistent solutions towards Android OS.

3.6. Summary

In this chapter the requirement analysis were approached in order to address all system behaviours and necessary features to the system. Thus, Section 3.1 presented the essential requirements, Section 3.2 and 3.3 focused and presented behavioural, interaction and sequence diagrams. Section 3.4 presented the used technologies in this work. Last, Section 3.5 presented some important aspects regarding the Google Android platform.

4. Ubiquitous Cryptographic Solutions

In this chapter it will be focused the two proposed cryptographic solutions, regarding cooperation mechanisms security in a mobile environment. Hence, due to the fact that the created solutions aim mobile applications with built-in cooperation mechanisms, those will be shortly introduced and described in Section 4.1. Then, in Section 4.2, the first proposed solution (DE4MHA) is presented followed by an enhanced solution of the previous one (eC4MHA) in Section 4.3.

4.1. Cooperation Mechanisms

Cooperation mechanisms aim to assure that users of an m-Health system without WiFi or cellular network data connectivity, can access remote data through cooperation, requesting packet forwarding from nearby nodes and receiving data through Bluetooth.

The cooperation strategy for m-Health applications with service oriented architectures (SOAs), is based on two mobile modules and one remote module: *i*) the node control message (NCM), *ii*) the requester control message (RCM) and *iii*) the cooperative web service (CWS).

The mobile nodes control messages aim to provide an awareness of the relay node status, i.e., if the node is willing to cooperate and in what conditions. It contains the established node unique identifier, the battery state, the Internet connectivity status, and the cooperation status (i.e., if its cooperative or not).

The requester control message is first sent by the initial requester node (mobile device with m-Health application requesting health data), and it comprises five main components: 1) the requester ID, the node unique identifier; 2) the service request, i.e., what the node is specifically requesting (e.g., the login token or its health profile); 3) the neighbours list; 4) the reputation list; and 5) the achieved cooperation time (ACT).

The network cooperative list illustrated in Figure 14 registers all cooperative and uncooperative network nodes throughout a service request. This list classifies all the neighbour nodes cooperative actions. It saves the Node ID and adds or subtracts a classification threshold according to the node cooperation status. When a service is requested from a node without Internet connectivity, all nodes update their status in the cooperative list.

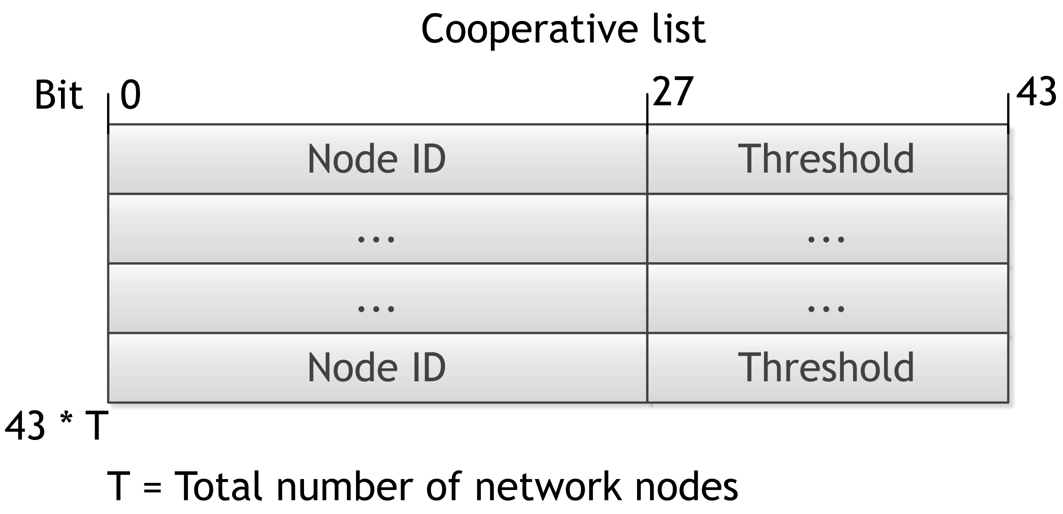


Figure 14 - Illustration of the cooperative list.

The cooperative threshold list (CT) influences directly the node reputation. The list starts at 0 (zero) and a unit (1) is added or subtracted according to the node cooperation status and node status. The correlation between the node cooperation status, the node status, its Internet connectivity and the resultant CT is it's an important point regarding cooperation among mobile nodes.

The node status is based on its storage capacity and energy lifetime. A node has three types of status: poor, regular, and excellent. A node with poor status is when the device storage capacity is over 95% or its available power energy is below 20%. The regular status when a node storage capacity is under 95% and its power energy is between 20% and 80%. A node is in an excellent status when the node storage capacity is under 95% and its available power energy is over 80%. The CT value guarantees that non-cooperative nodes are punished.

The cooperative Web service (CWS) includes and manages the node reputation table. To calculate nodes reputation, the CWS uses the cooperative lists deciding if the requesting node should have access to the m-Health application WS or not.

Based on nodes reputation, the CWS will not grant access and release any resource from the WSs to selfish nodes. Selfish nodes are punished by the CWS with an order to cooperate until its reputation reaches a cooperative state. The CWS must always release resources to cooperative nodes, however, super-cooperative nodes have a maximum priority in case of simultaneous requests. Figure 15 presents a user scenario of the m-Health cooperation approach. User A has network connectivity and cooperates, the status value is according to the battery status. User B has network connectivity and does not cooperate. Then, the status value will suffer a negative impact according to the battery status. Users C and D do not have network connectivity. User C queries User A for cooperation and receives a positive response and all the requested data. User D queries User B for cooperation and receives a negative response. Then, User D requests data from User C that answers this request, getting positive status by cooperating.

Cooperating nodes have a better reputation, and have priority over selfish nodes to access the m-Health application services.

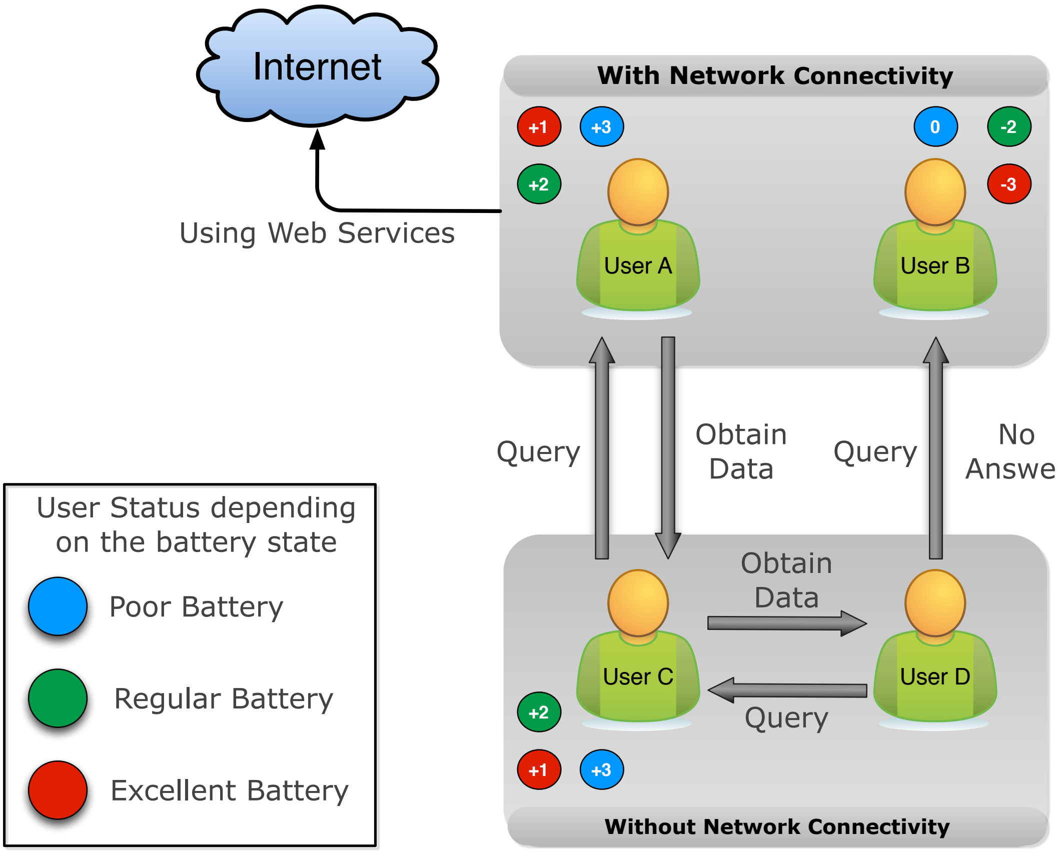


Figure 15 - Illustration of the interaction for an m.Health application with the cooperation approach for 4 users.

Hence the main objective of cooperation mechanisms is to assure that all users of a service-oriented mobile health application, regardless of their connectivity options (i.e., if they have or do not have Internet connectivity through WiFi or cellular network), can accomplish a request for a service and retrieve remote health information.

4.2. Data Encryption for Mobile Health Applications (DE4MHA)

This section presents the data encryption proposal for mobile health applications (DE4MHA) in cooperative environments. The main goal consists in assuring and guarantying m-Health data confidentiality, integrity and authenticity in a cooperation environment, where sensitive and personal data is exchanged through several different agents. It is important to refer that this proposal focuses essentially on protecting data while being transmitted over the network, instead of considering the privacy and protection of data stored on mobile devices.

Hence, data exchange among nodes must be accomplished through encryption techniques, to protect sensitive data from being disclosed to unauthorized entities. Two distinct possibilities are available for such objectives, namely symmetric and asymmetric algorithms. Chapter 2 addressed this thematic approaching the pros and cons of each technique. Therefore DE4MHA uses a hybrid approach in which asymmetric algorithms are used for session key exchange and symmetric ones are used for encrypting data transferred among nodes on the network.

The DE4MHA begins with a mobile node (a person using SapoFit), trying to access the SapoFit WS that contains the user profile, weight measures, fitness and diet indications. A SapoFit user (mobile requester node) without network connectivity and therefore without access to the SapoFit WS, will try through cooperation to obtain the required health information. For that, another user with network connectivity (mobile requested node) and with integrated cooperation mechanisms will forward the requested health information from the SapoFit WS. Both the requested and requester nodes will exchange (through Bluetooth) a public key message (PKM). After the public key exchange, the requested node creates a session key, encrypting it with the requester node's public key. Then a signature of the whole message is created and appended to the session key message (SKM) that is sent to the requester node. When the message is received, containing the session key, if its integrity and authenticity is verified, the requester node sends an acknowledgement (Ack) to the requested node. This method guaranties safe communication between nodes, otherwise if the integrity and authenticity is not verified, the communication between nodes is ended. A mobile node with network connectivity will access the cooperative WS to obtain the required health information. To secure all communication between the WS and the requested node, the secure socket layer (SSL) over the HTTP (also known as HTTPs) is used. Through SSL all retrieved health data from the WS is properly encrypted to assure maximum confidentiality of transmitted data.

It is important to refer that DE4MHA focuses on a peer-to-peer node-forwarding scheme based on node reputation, with encryption/decryption tasks on each node, limiting WS access to nodes with low reputation value. Each cooperative node encrypts and decrypts received messages until it reaches a node with Internet connectivity, what makes necessary that each mobile node possesses a session key agreed with the mobile node with which is communicating. Figure 16 illustrates the overall behaviour of DE4MHA and the most fundamental messages exchanged between two mobile nodes, that requires safe communication establishment in order to exchange information through cooperation. It essentially lies down to a requester node trying to obtain data through cooperation, performing the process of node discovery, and further connection through Bluetooth to a mobile node willing to cooperate (1). When both nodes are connected through Bluetooth, both nodes will generate a RSA key pair, exchanging their public key, so that each mobile node will be able to encrypt messages for later exchange (2). As soon as the requested node receives the requester node’s public key, it proceeds to generate an AES session key with 128 bits size, encrypting it through the requester node’s public key, appending then a digital signature to assure data integrity as well authenticity (3). Finally, if the previous message is received by the requester node, its integrity and its authenticity will be checked and if nothing wrong happened, the requester node will create an Ack message, and a signature to guaranty that requested nodes know that the requester node has properly received the session key (4). Therefore, all exchanged messages will be encrypted using the referred session key instead of the key pair used to exchange the session key, due to the superior time taken to encryption/decryption procedures by public key cryptography.

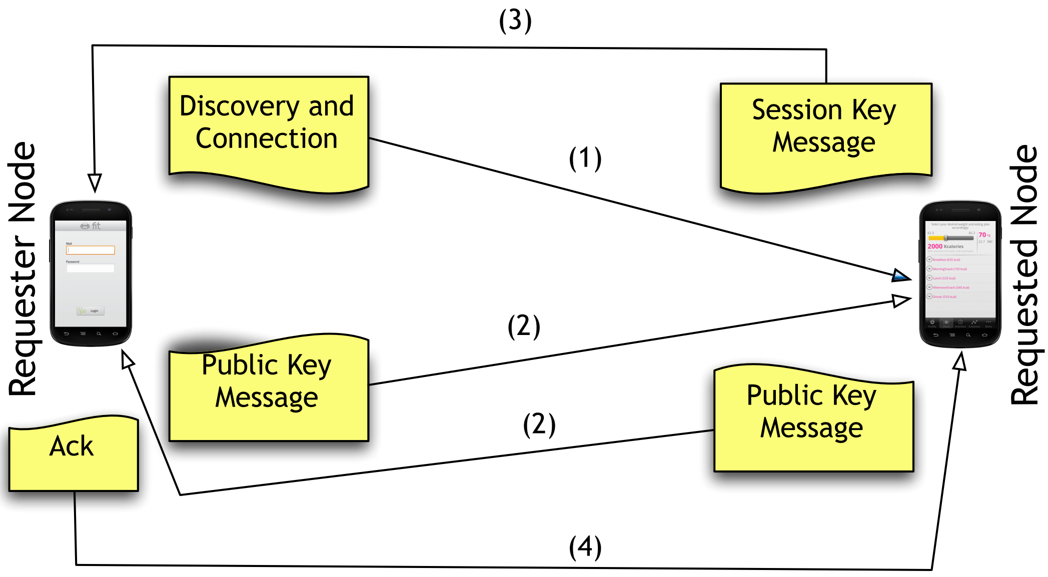


Figure 16 - Data exchange sequence.

4.2.1. Public Key Message

Public key messages are sent from both requested nodes to requester nodes and aim to provide to each node their public key. This public key is used whenever it is required to encrypt a session key and send it afterwards, enabling safe session key transfer. If two mobile nodes in need to establish a safe connection already own opposites public keys, an exchange of a public key message is avoided, resulting in an improvement of efficiency regarding the time necessary to gather all requisites to safe exchange information.

Figure 17 illustrates the public key message. The two following modules comprise the public key message:

- Node unique ID: This identifier it is arranged through an aggregation of the mobile device Bluetooth mac address and the user unique identifier.

- Public Key: In this element will be placed the RSA public key previously generated along with the necessary private key.

These two elements comprise the public key message, which essentially enables safe session key exchange among mobile nodes on the network. It is important to notice that all content inside of a public key message is carried through the network in plain text, due to the fact that public keys are intended to be public and made available to everyone.

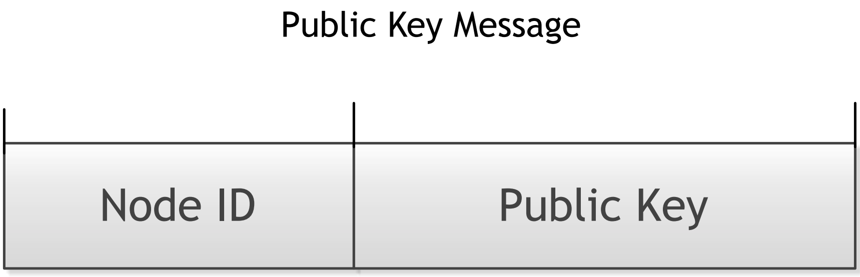


Figure 17 - Public Key Message.

4.2.2. Session Key Message

The requested node is the one who sends the session key message and it comprises three main components: (1) the requested ID, (2) the session key and (3) the signature. The three main components of the session key message are illustrated in Figure 18 and may be described as follows:

- Requested ID: As previously referred, the requested ID results from the aggregation of the mobile device Bluetooth mac address and the user unique identifier.

- Session Key: In this field will be placed the session key used to encrypt and decrypt all data flowing among mobile nodes on the network, assuring that all sensitive data is kept safe and its content remains unknown to unwanted threats, ensuring this way confidentiality.

- Signature: To every message exchanged between mobile nodes, an hash of that message is generated, being then encrypted with the node's private key creating this way a signature of the message. It will enable the receiver node, in this particular case, the requester node, to assure that the message is exactly as it was when it was sent, i.e. its integrity remains intact, and at the same time it assures that the message was sent from the expected person (mobile node), i.e., guarantees authenticity.

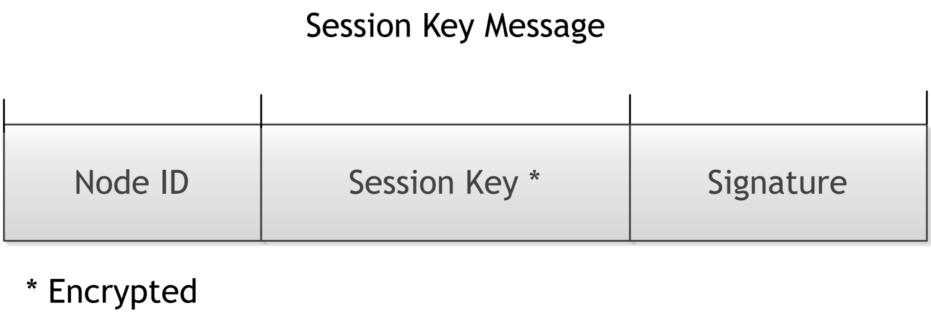


Figure 18 - Session Key Message.

When the requester node receives the session key message from the requested node, it verifies its integrity and authenticity. If the message has not been corrupted, neither sent by someone else other than expected, both the requester and requested nodes can from this moment on safely communicate and exchange messages, using the session key that only both possess in common.

4.2.3. Symmetric Algorithm Choice

In order to choose the most suited symmetric encryption algorithm for DE4MHA, performance tests were conducted using four different encryption algorithms, namely AES, TripleDES, RC4 and Blowfish. The choice fell on these algorithms given the results registered and observed in the literature. Given that DE4MHA aims any mobile health application in a cooperative environment, therefore not knowing a priori the amount of data that each application usually handles, different sizes of data that should be encrypted have been used as a performance metric.

As may be seen in Figure 19, results shown that when data size to encrypt grows, the encryption time (seconds) also increases, as expected. When comparing small amounts of data, all four algorithms presented similar results. However AES algorithm presented better results, since the encryption time of larger data tends to grow up very slowly. The other three tested algorithms all tend to grow up exponentially as data size to encrypt overcomes 1000KB. The 3DES algorithm presented the maximum observed encryption time, encrypting 10000KB of data, which took on average 14.3 seconds. With the same amount of data the AES encryption time was only 0.0045 seconds.

Regarding decryption (Figure 20) similar results were obtained in comparison to encryption, i.e., all four tested algorithms presented nearly the same performance, achieving identical encryption/decryption times. Once again, AES algorithm took advantage over the other used algorithms, revealing the best performance in the conducted trials. AES algorithm presented a decryption time of average 0.0038 seconds to decrypt 10000KB of data, while in the worst-case scenario, 3DES algorithm presented the worst results observed.

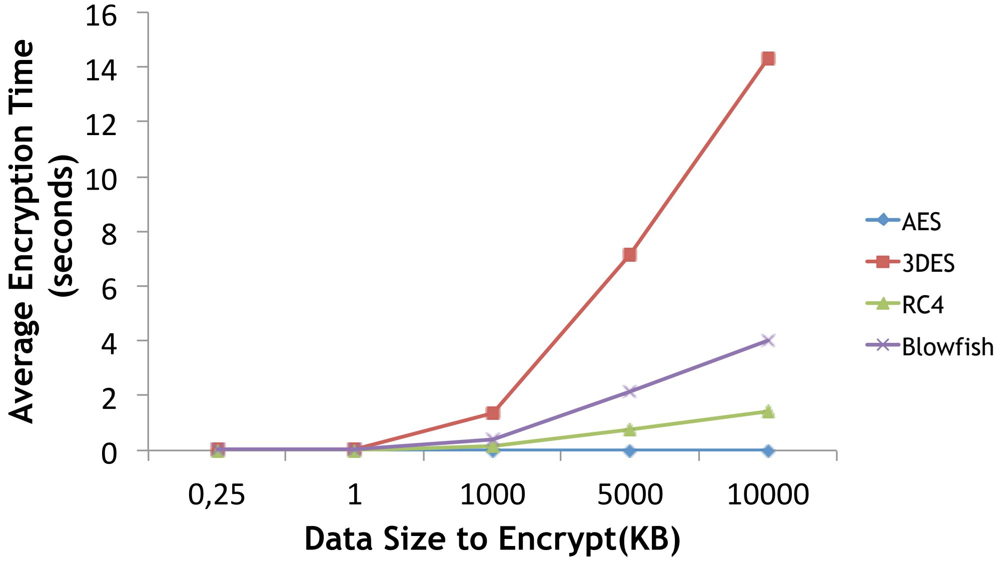


Figure 19 - Average Time Encryption.

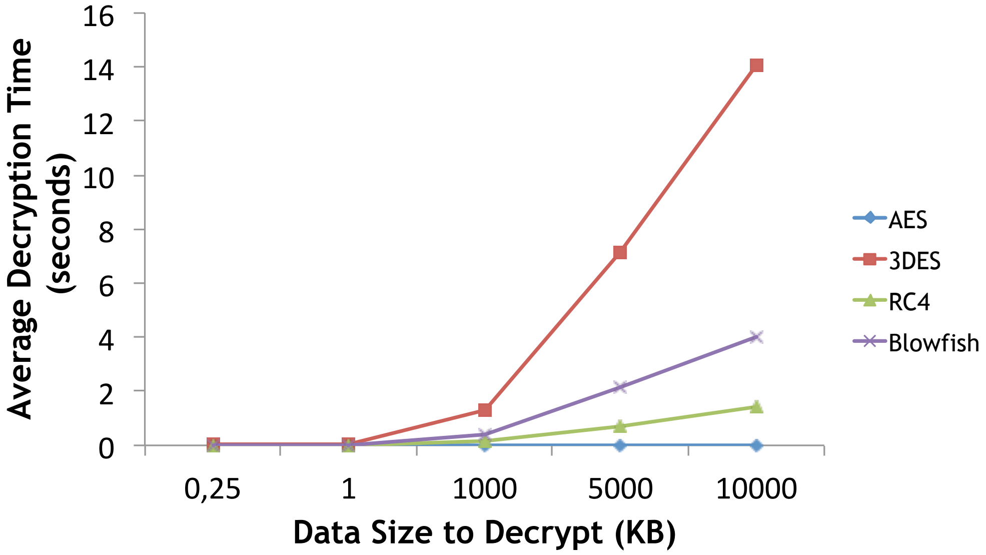


Figure 20 - Average Time Decryption.

Given the previous results obtained, AES algorithm was chosen to be the one operating on DE4MHA as a symmetric algorithm.

4.2.4. Asymmetric Algorithm Choice

Concerning the choice of an asymmetric algorithm in order to exchange session keys between mobile nodes, three options were taken in account, the RSA, Elgamal and the Diffie-Hellman algorithms. While RSA and ElGamal operate on the same base, i.e., through message encryption, Diffie-Hellman allows users to share a secret, generating then a session key based on the shared secret.

Given that RSA algorithm has the possibility of using it not only for encryption, but also to perform digital signature, it was the chosen one in detriment of Elgamal and Diffie-Hellman, using it as a two-in-one algorithm.

4.2.5. Integrity and Authenticity

In order to assure integrity, message digest 5 (MD5) algorithm was chosen. It takes as input a message of arbitrary length and produces as output a 128-bit “hash” value or “message digest” of the input. When used multiple times with the exactly same message, it should always produce the same hash value. This way, if a message is modified or corrupted, by generating an hash value and comparing it with the original one, it is possible to verify if the message hasn’t been corrupted, i.e., if maintains its integrity.

On the other hand, to guarantee authenticity, two approaches were taken in account, namely (1) using RSA algorithm to encrypt the hash value previously generated with MD5 and (2) using DSA, but unlike RSA it can only sign and can not encrypt information. Since a hybrid approach has been chosen, where AES is used for symmetric encryption and RSA used for asymmetric encryption, the last one was chosen to perform digital signature, taking in advantage the fact that RSA will be used both for session key exchange and digital signature performance. Thus, there's no need for generating a pair of keys to exchange session keys, and another one for digital signature, avoiding reducing the efficiency of the proposal.

DE4MHA is presented as a solution to assure confidentiality, integrity and authenticity of the data that is typically carried in m-Health applications with built-in cooperation mechanisms. It essentially focuses on forward health data between cooperative mobile nodes encrypting it from cooperative node to cooperative node, until reaching a web server (in a request scenario) or a mobile node (in a response scenario).

4.3. Enhanced Cryptography Solution for m-Health Applications in Cooperative Environments (eC4MHA)

This enhanced proposal called eC4MHA, focuses on enhancing the previous proposed solution for m-Heath applications in a cooperative environment. Thus, it overcomes the above-mentioned limitation that includes nodes forwarding messages, performing encryption/decryption tasks in each node. Furthermore, mobile nodes act merely as messages forwarders. They do not perform encryption tasks (except on the requester node and in the Web server), what contributes to increase the overall network performance in comparison to DE4MHA.

4.3.1. Assuring Data Confidentiality

To assure this property and as it happened in the previous proposal, two approaches were considered, 1) using only asymmetric cryptography, and 2) a hybrid approach using both asymmetric and symmetric cryptography. The first approach considered the utilization of RSA algorithm with a 1024 bits key size on both mobile nodes and the WS itself. After public key exchange between the WS and a mobile node, all the exchanged information would be encrypted on the sender's side with the receiver's public key and decrypted with the receiver's private key. Although this option is completely valid to specific scenarios, it is necessary taking into account that RSA algorithm can only encrypt a limited amount of data that is directly related to the public key size. For instance, a 1024 public key can only encrypt 117 bytes, i.e., (1024/8) - 11 bytes.

The eC4MHA proposal aims any m-Health system, including applications that handle different amounts of data. Hence, this approach was not feasible and was discarded.

The second considered and applied approach in eC4MHA, is based on using a hybrid scheme to perform data confidentiality. The AES symmetric algorithm was chosen to encrypt all the data and the RSA asymmetric algorithm was used to exchange a random secret key used by the AES algorithm (previous performance evaluations regarding symmetric algorithms were taken into account, hence the choice of the AES algorithm). It is assumed that a user is able to access directly (through Internet connectivity) the m-Health application WS. The reason for such assumption is the required exchange of the secret key between the WS and the mobile node before encryption can be performed, as may be seen in Figure 21.

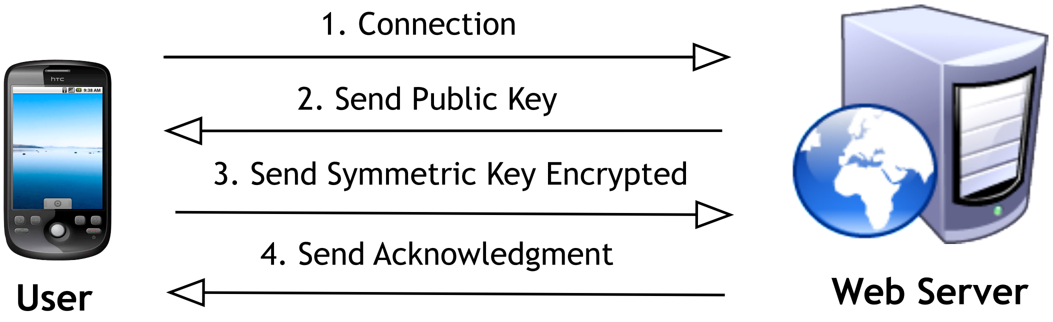


Figure 21 - Illustration of key exchange sequence on eC4MHA.

From this moment on, the user is able to securely retrieve health data, whether cooperation is required or not. Thus, the applied strategy assumes a secure transaction of data between nodes and the WS using the AES encryption algorithm in Cipher Feedback Mode (CFB), with a key size of 128 bits, and RSA algorithm with a 1024 bits keys size to exchange secret keys between nodes, and the WS.

4.3.2. Integrity and Authenticity

To assure authenticity, eC4MHA uses MD5 algorithm in order to produce a 128 bits output, called message digest. To guarantee integrity, it uses the RSA algorithm to encrypt the message digest, commonly known as digital signature. The digital signature is then appended to the message that should be sent over the network.

Under this approach, cooperative mobile nodes should not know personal information that is being carried by messages sent all over the network, namely, the requester control message that contains user access credentials, such as username or password. A cooperative mobile node will merely act as a packet forwarder, until it reaches a mobile node with Internet connectivity. The mobile node is not aware of the packet content, other than required cooperative data, such as node identification, in order to forward back the response or reputation lists (RLs), determining and updating the level of cooperativeness of each mobile node. Through this proposal, it is assured that none of the sensitive information, such as login tokens or user's health information, is disclosed to unauthorized persons. Furthermore, it guarantees that information received is the original one as well as it comes from an expected and reliable source. Otherwise, an alert message is displayed on the mobile device, informing the user that something went wrong, while trying to retrieve health data through cooperation.

4.3.3. Key Management

Cryptography algorithms require encryption/decryption keys to operate. Consequently, it is vital to assure key's protection and privacy. This fundamentally depends on two factors, namely, where the keys are stored and who has access to them [101]. eC4MHA uses a *keystore* to store and assure key's protection and privacy. As above-mentioned, it is necessary to establish a previous connection to the WS in order to exchange a secret key for later communications. After the secret key generation, a *keystore* is created and the key is then securely stored and protected with a user password in the mobile device. To retrieve the secret key, the user must provide a password (in a transparent manner). Although the secret key is physically present in the device, it is not possible to access it from another application other than the application used to store the key. As for the WS, a *keystore* is also generated and used to store its own private key and each secret key needed for each node that requests data.

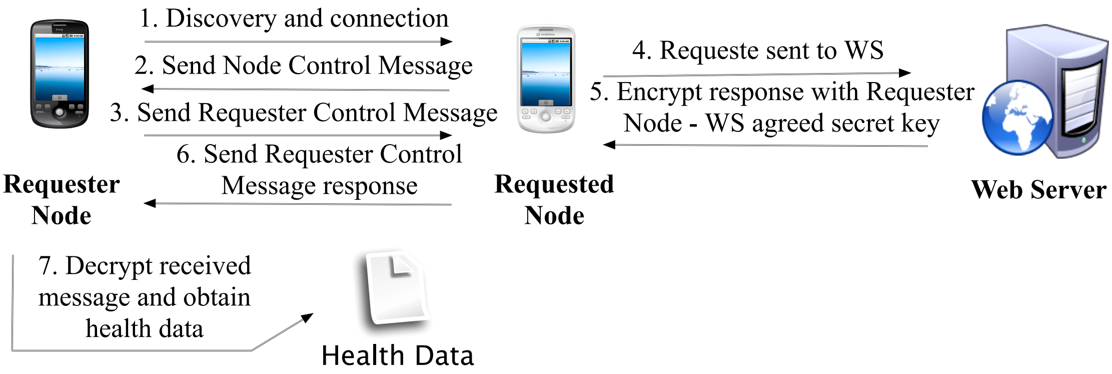

1. Discovery and connection
2. Send Node Control Message
3. Send Requester Control Message
6. Send Requester Control Message response
Requester Node
Requested Node
4. Requeste sent to WS
5. Encrypt response with Requester Node - WS agreed secret key
Web Server
7. Decrypt received message and obtain health data
Health Data

Figure 22 - eC4MHA typical workflow.

Figure 22 presents the overall and usual workflow of the eC4MHA in a cooperative environment. As may be seen, a requester node will try to discover and establish a connection to a mobile node through the above-mentioned cooperation mechanisms, receiving then a node control message. Then, a requester control message is sent to the requested node in order to define what information is it requiring. All the sensitive data is encrypted and signed. The requested node will then forward the request to the WS. The WS will receive the data, encrypting and signing it. The response is sent back to the request node forwarding it to the requester node that, after decryption, message integrity, and authentication verification will obtain the requested data.

4.4. Summary

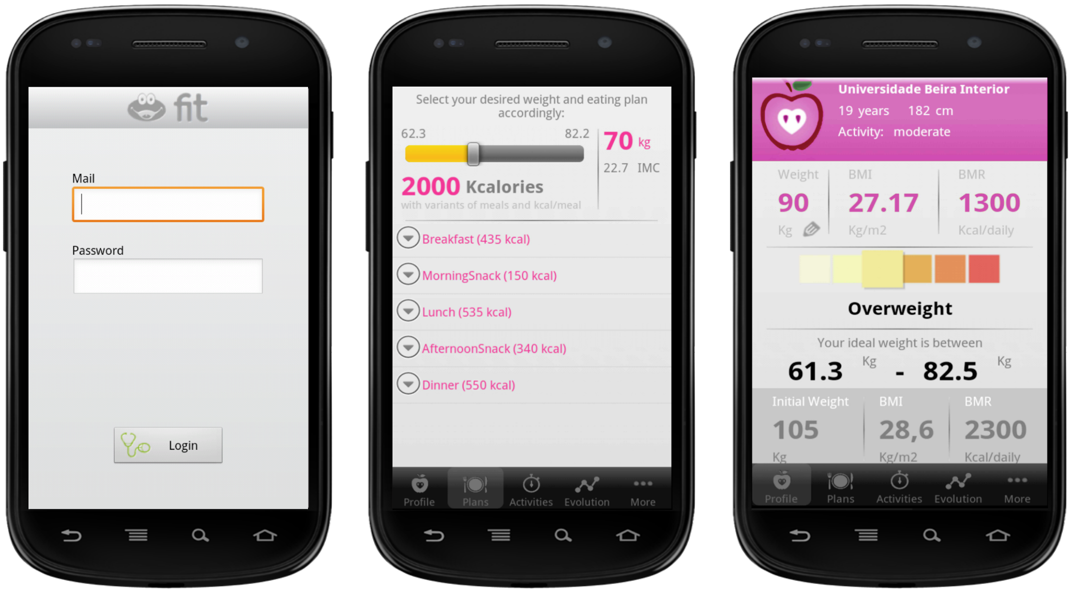
In this chapter it was shortly presented in Section 4.1 the cooperation mechanisms for which the cryptographic mechanisms were developed. In Section 4.2 and 4.3 were presented the architecture of the two considered and developed solutions, namely DE4MHA and eC4MHA respectively. Thus, the main objective of this chapter was to present two robust and reliable solutions that allows secure health data exchange in mobile health applications with cooperation mechanisms embedded. This is achieved through cryptography, by assuring three of the most fundamental properties concerning data security, i.e., data confidentiality (through encryption), data integrity (through hash functions) and authenticity (through digital signature). All these properties contribute to a more reliable and secure way of exchanging information with security.

5. Performance Evaluation and System Validation

This section focuses on the performance evaluation and validation of the cryptographic solutions developed for m-Health application with built-in cooperation mechanisms. First, the m-Health application (SapoFit) and corresponding network scenario used to evaluate and demonstrate the solutions are introduced. Afterwards, the system validation and results are discussed for both approaches, concluding with a comparison between the two proposed solutions.

5.1. SapoFit Application

SapoFit is a weight control mobile health application that allows users to keep track of weight in a healthier and more practical way. SapoFit allows users to control their weight, body mass index (BMI), basal metabolic rate (BMR), sports activity, and the possibility to follow food plans based on their needed calories. In this m-Health application, all the users must be registered in a Web service. Figure 23 presents the three main activities screenshots of SapoFit application: Login, Plans, and User Profile.



Select your desired weight and eating plan accordingly:

62.3 82.2 70 kg

22.7 IMC

2000 Kcalories

with variants of meals and kcal/meal

Breakfast (435 kcal)

MorningSnack (150 kcal)

Lunch (535 kcal)

AfternoonSnack (340 kcal)

Dinner (550 kcal)

Universidade Beira Interior

19 years 182 cm

Activity: moderate

Weight 90 Kg | BMI 27.17 Kg/m2 | BMR 1300 Kcal/daily

Overweight

Your ideal weight is between

61.3 Kg - 82.5 Kg

Initial Weight 105 Kg | BMI 28,6 Kg/m2 | BMR 2300 Kcal/daily

Figure 23 - Three main activities screenshots of SapoFit application: Login, Plans, and User Profile.

The proposed cryptographic solutions were integrated and deployed in this Android m-Health application with cooperation mechanisms embedded working ubiquitously, as previously referred, for test and evaluation purposes. The application with cooperation mechanisms on its essence uses a Web Service to remotely store and retrieve all user information, which was modified in this work to provide the cryptographic features to the WS.

5.2. M-Health Network Scenario

An illustration of the real network scenario used for the performance evaluation study of both DE4MHA and eC4MHA may be seen in Figure 24. It includes seven mobile nodes (using SapoFit), where three of them are assumed to be uncooperative nodes. Node M is the only node with available connection to the SapoFit Web service. Although this scenario may present mobility issues, for evaluation purposes, it is considered that each mobile node assumes the position presented in the network scenario.

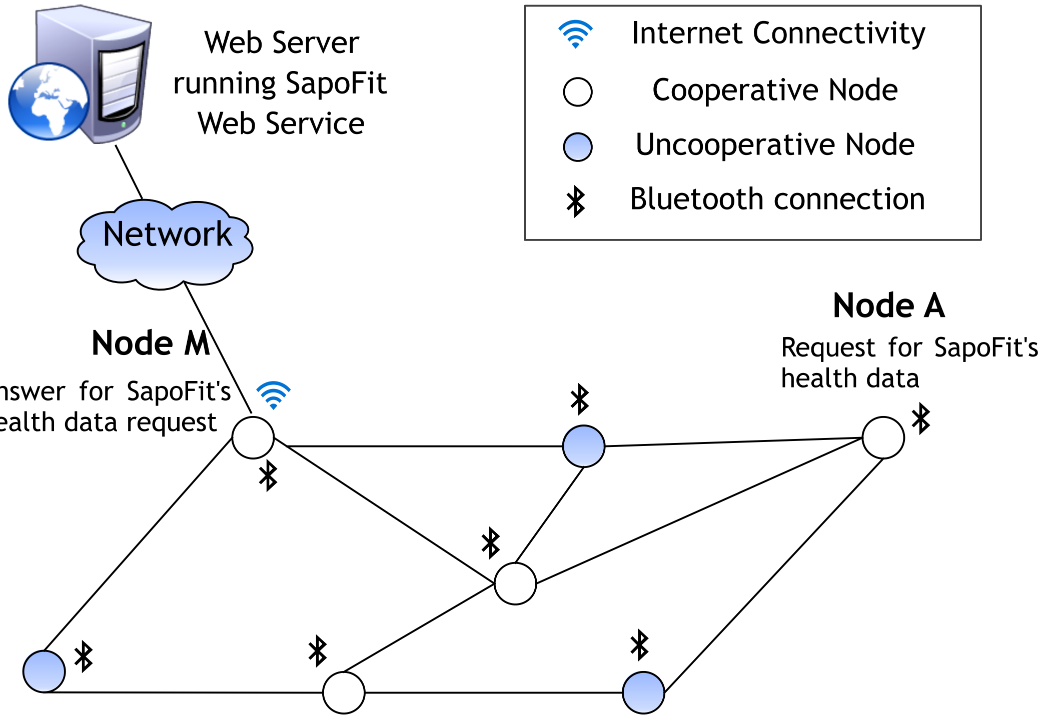


Figure 24 - Illustration of the network scenario for performance evaluation of the eC4MHA.

In the presented scenario, all the devices have Bluetooth class 2 modules, but only one device has Internet connectivity. Users without Internet connectivity must use the integrated cooperation mechanisms in order to obtain the requested health information. When the number of uncooperative nodes increases, the average time of any request or response also naturally increases.

Non-cooperative cases where controlled and measured to a maximum of three to guarantee the minimum service performance. Through cooperation all the devices can indeed use the m-Health application. However, uncooperative nodes affect directly the service delivery probability.

The performance evaluation was carried using seven real mobile devices as may be seen in Figure 25, where three of them served as uncooperative nodes, with different hardware and software used with the SapoFit m-Health application.

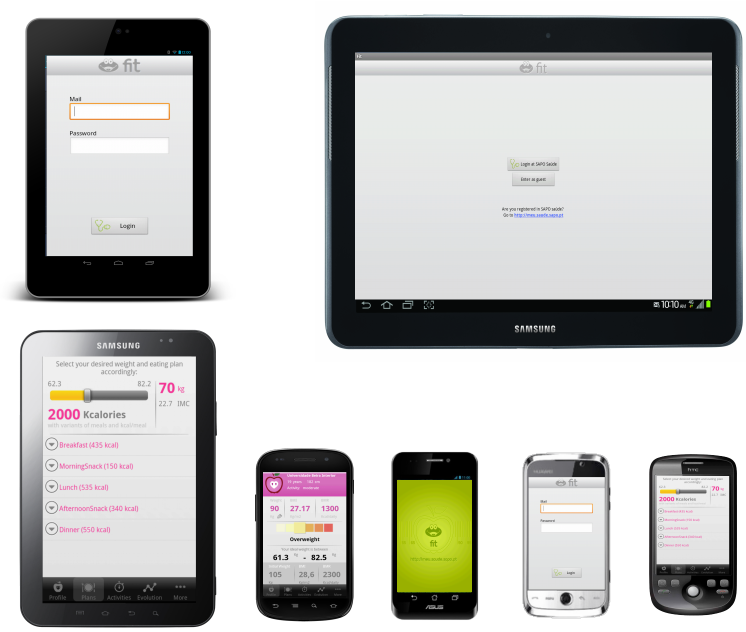


Figure 25 - Mobile devices used for trials with the SapoFit m-Health application.

The seven mobile devices, three tablets and four smartphones have the Google Android Operating System, with the 4.0.4 version on the Samsung Nexus S, Asus Padphone 1, Samsung Nexus 7 as well on the Samsung Tab 10.1. Android version 2.3.3 is present on all left devices, i.e., on HTC Magic, Huawei A1 and Samsung Galaxy. As mentioned-above, these devices possess Bluetooth class 2 modules, as most of the common mobile devices [102], and the 2.1 core version. Bluetooth class 2 means that these devices have an approximate maximum range of ten meters.

Next section presents the perform evaluation of both DE4MHA and eC4MHA individually, as well a comparison between both solutions.

5.3.Performance Evaluation of DE4MHA and eC4MHA

This section carries the perform evaluation of DE4MHA and eC4MHA individually, presenting the performance metrics which will then be used to evaluate the system performance in Section 5.3.1. Thus, performance metrics considered in this study are the service delivery probability (in percentage) and the service average delay (in seconds). The service delay is measured as the time between the request and its corresponding response, while the service delivery probability consists on the rate of successfully responses originated by mobile nodes requests. This section finishes with a comparison between DE4MHA and eC4MHA, using the previous performance metrics to assess which solution presented the best results.

In order to efficiently evaluate the performance of both proposals, and to have an awareness of a comparison term, i.e., the means to evaluate how cryptographic mechanisms affect the performance of the cooperation mechanisms (although adding a robust layer of security), it was considered to use previous performance metrics tested in the application with cooperation mechanisms embedded and then use the same proposed metrics in the exact same application with cooperation mechanisms built-in, but unlikely the former, with the proposed cryptographic solutions already incorporated, namely DE4MHA and eC4MHA proposals.

5.3.1. DE4MHA Performance Analysis

The service delivery probability and the service average delay in function of the number of uncooperative mobile nodes in both scenarios (with and without cryptographic solutions) regarding DE4MHA are presented in Figure 26 and 27 respectively.

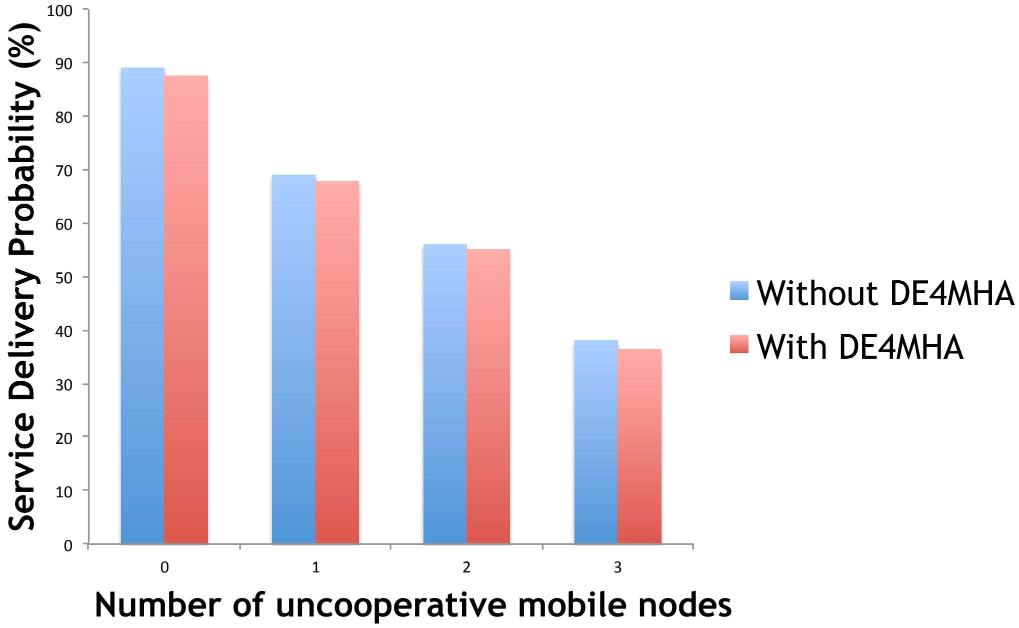


Figure 26 - Service Delivery Probability with and without DE4MHA.

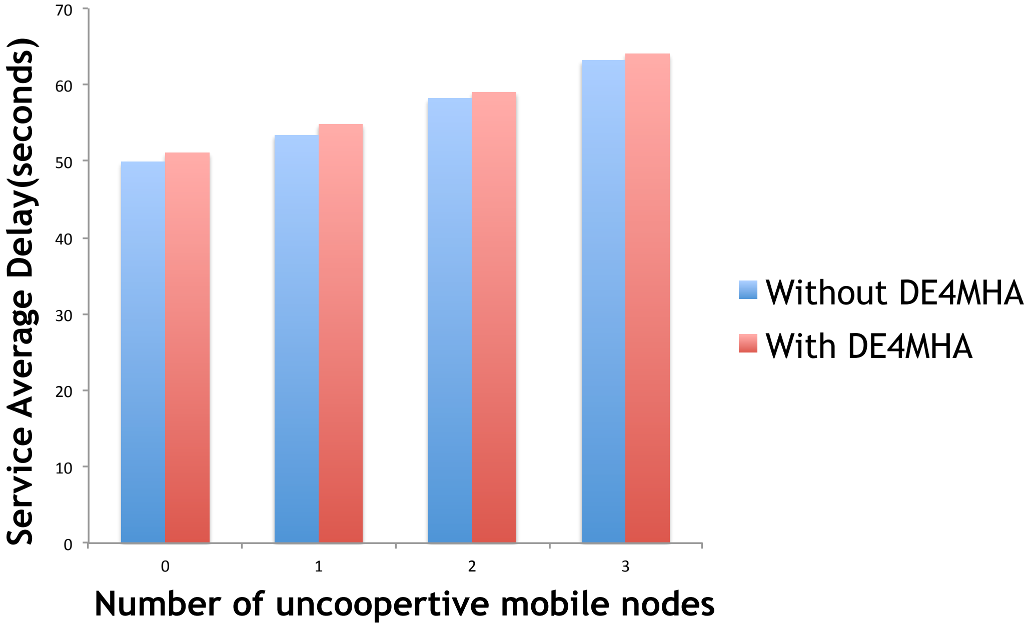


Figure 27 - Service Average Delay with and without DE4MHA.

As may be seen in Figure 26, the probability that a request is successfully answered in function of uncooperative nodes in the network decreases with the increasing of uncooperative mobile nodes. This is due to the fact that uncooperative nodes do not forward request or response messages. Taking into account, performed tests with and without DE4MHA, slightly worse results were observed with DE4MHA. The service average delay also grows as the number of uncooperative mobile nodes increases, as expected, observing also a slightly, but almost insignificant worse result when DE4MHA solution is present. Results show a minimal increase of the overall time taken to accomplish cooperation tasks when cryptographic mechanisms are present (e.g., encryption tasks or encryption keys exchanged between mobile nodes), not compromising the overall network performance. Hence, due to DE4MHA incorporation, the average time added with cryptographic tasks corresponds to approximately 0,003557 seconds, and if compared with the average time taken by isolated use of cooperation mechanisms, it corresponds to an increase of 2% of the overall time. In this sense, the extra time required is perfectly acceptable since privacy and security is a concerning issue and nowadays a “must-have” in every m-Health application. This minimal increase of observed overall time to accomplish tasks when cryptographic solutions are present might be explained for two different reasons. The first one regards the evolution of mobile nodes in what processing capability respects, presenting nowadays a remarkable growth in this area. The second one, may be explained to the remarkable efficiency of the AES algorithm, which is used in this proposal to encrypt every communication between mobile nodes evolving any data transmission other than encryption keys, coupled with the fact that SapoFit usually handles a small amount of information. However and as illustrated on Chapter 4, AES algorithm presents real decent and satisfactory results when handling with both small and greater quantities of data to accomplish encryption tasks.

5.3.2. eC4MHA Performance Analysis

To measure the perform evaluation of eC4MHA, the previous performance metrics were considered and the results may be observed at Figure 28 and 29, presenting the service delivery probability and the service average delay respectively.

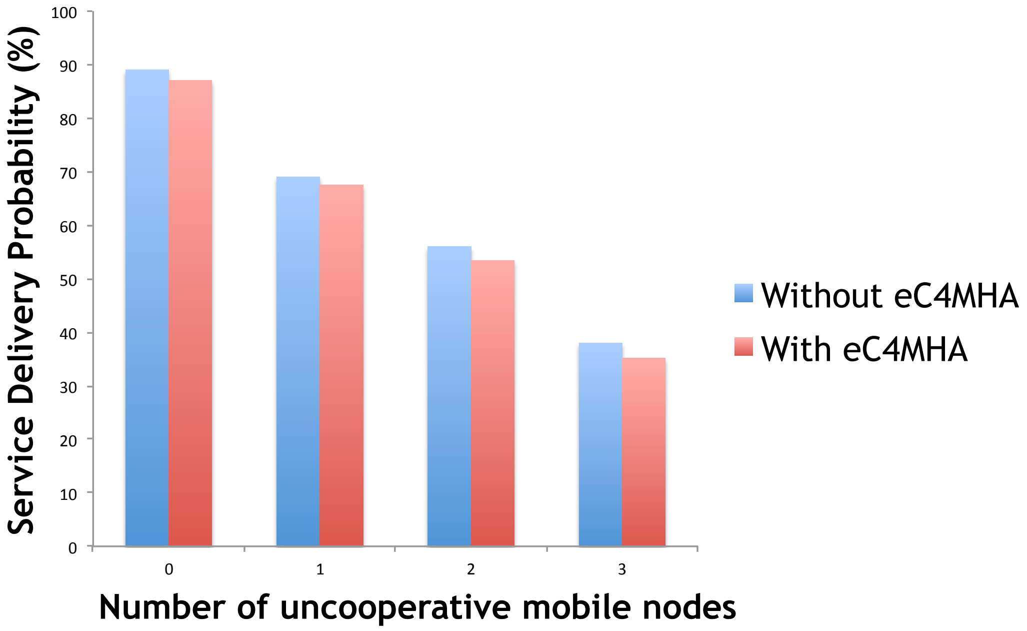


Figure 28 - Service Delivery Probability with and without eC4MHA.

Figure 28 shows that cryptographic algorithms degrade slightly the overall performance, as expected and already observed with DE4MHA, due to more time consuming tasks, such as encryption and decryption. However, the service delivery probability presents similar results with cryptographic algorithms. The variance reflects the use of eC4MHA in cases where whether integrity or authenticity is not guaranteed, resulting in a denial of service to the initial request, besides the fact that uncooperative nodes also contribute to this registered variance. Therefore, it contributes to the decrease of the service delivery probability. When there are no uncooperative nodes on the network, a rate of 89% of service delivery probability is registered while with eC4MHA a rate of 87.5% is achieved. In the worst-case scenario, eC4MHA presents a rate of 36.4% of delivery probability, as opposed to a rate of 38% without eC4MHA.

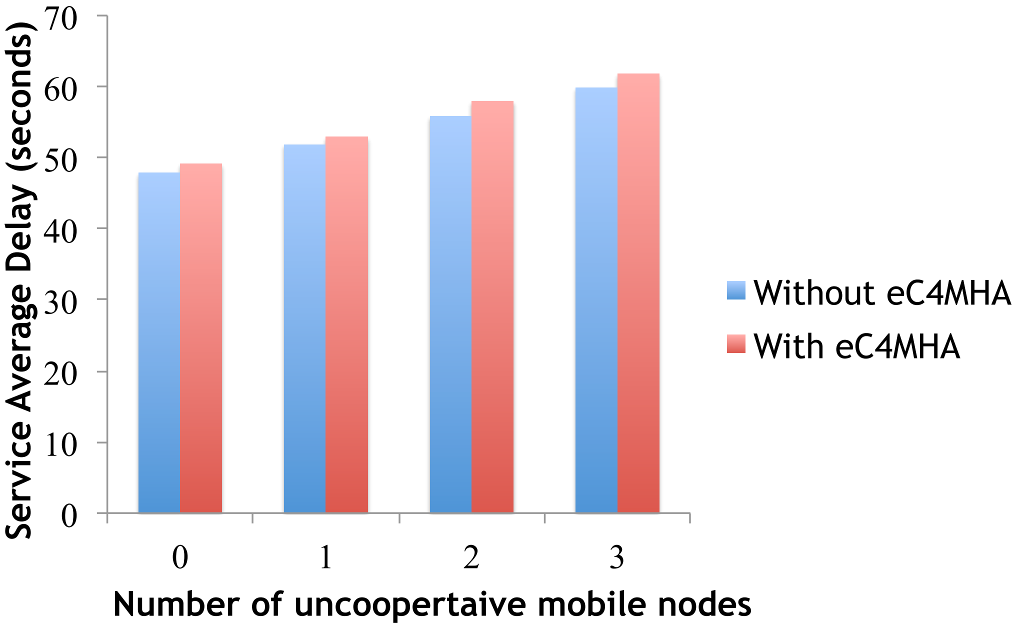


Figure 29 - Service Average Delay with and without eC4MHA.

The maximum service delay observed with three uncooperative nodes was about 59.8 seconds without eC4MHA and about 61.8 seconds with eC4MHA. These main variances were mostly caused by mobile devices constraints, such as loss of Bluetooth connection or distance variations among mobile nodes.

5.3.3. DE4MHA and eC4MHA Comparison

A performance evaluation analysis with the comparison of both cryptographic solutions for m-Health applications, DE4MHA and eC4MHA was also considered and studied (Figure 30 and Figure 31). Measuring the service average delay with both approaches, it was demonstrated that eC4MHA is more efficient and it has better overall performance over DE4MHA. Significant changes were made to the previous proposed solution, considering that each cooperative node would have to encrypt and decrypt data, by make them acting uniquely as packet forwarders in this new approach. Results show a slight improvement in the performance of service average delay with the eC4MHA. In a worst case-scenario with three uncooperative nodes, the requester node would receive the response to the request in about 64.06 seconds with DE4MHA, while with eC4MHA an average of 61.8 seconds would be necessary in order to receive the response.

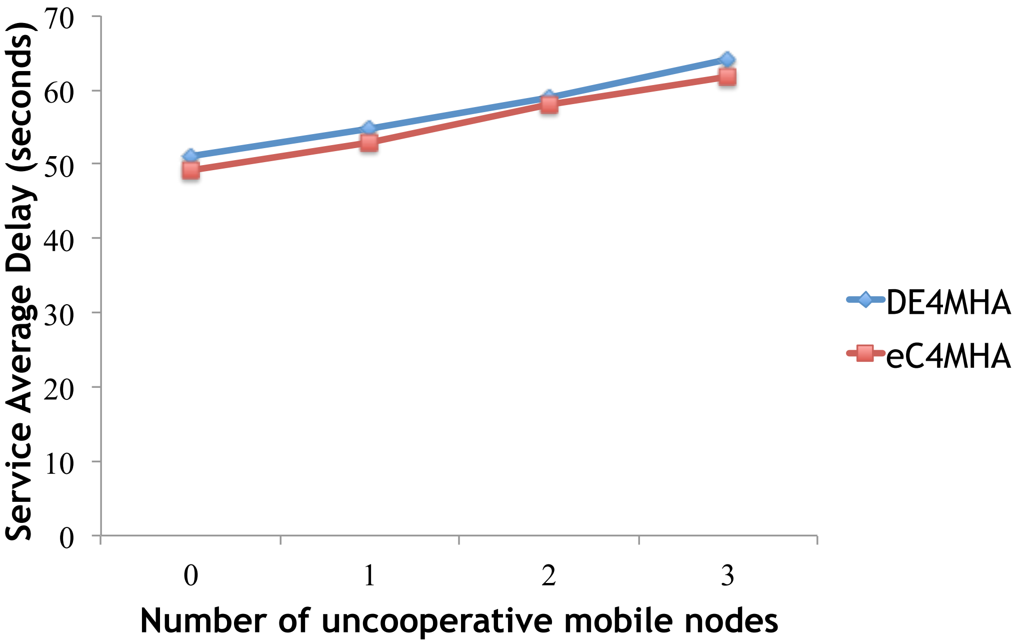


Figure 30 - Service Average Delay with DE4MHA and eC4MHA.

When comparing service delivery probability, both approaches presented similar levels of delivery probability. With zero uncooperative mobile nodes, DE4MHA presents a delivery probability of 87,5% while eC4MHA obtains a minor result, i.e., 87,1%. Bluetooth failed connections, corrupted messages, resulting in a denial of service due to the compromising of messages integrity, explain why a rate of 100% is not achieved when there is no uncooperative mobile nodes on the network, as opposite to the cases where uncooperative nodes are present, which contributes in a much larger scale to the decrease of registered rates and why it decreases when uncooperative nodes increase.

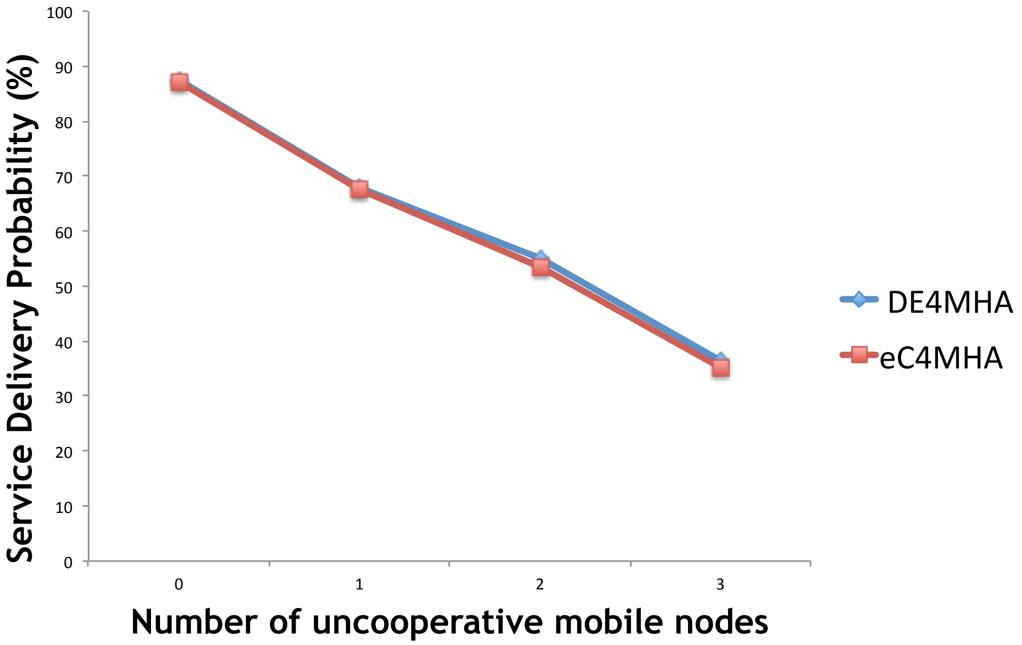


Figure 31 - Service Delivery Probability with DE4MHA and eC4MHA.

5.4. Summary

This chapter presented in Section 5.1 the m-Health application where the cryptographic mechanisms were integrated, namely the SapoFit application. This application, which was carried out by SAPO and NetGNA, aims the obesity prevention and treatment through a service oriented architecture. In Section 5.2, the network scenario was presented in order to provide an awareness of how the tests were performed. Section 5.3

presented the performance analysis of DE4MHA and eC4MHA based on two performance metrics, the service delivery probability (in percentage) and the service average delay (in seconds). Results clearly show that although a minimal increase of time is required in comparison to the original solution, where there are no cryptographic solutions, that fact becomes irrelevant due to the overall security added with the incorporation of such mechanisms. Last, a comparison between the two solutions was approached, which revealed that eC4MHA presents better results than DE4MHA, resulting in an improvement concerning DE4MHA.

6. Conclusions and Future Work

6.1. Conclusions

This chapter presents a synthesis of this dissertation along with the main achievements that result from this work. It also points some directions for further work. The main objective of this dissertation was the study of cryptographic mechanisms application on m-Health applications with built in cooperation mechanisms. In short, these cryptographic mechanisms aimed to assure that user's health data was kept safe and undisclosed to unauthorized entities mainly due to the sensitive data that these types of applications may carry (e.g. HIV disease information). After studying several cryptographic approaches, a requirement analysis in order to fetch all the systems analysis was conducted. Then, two different solutions were proposed, deployed, and evaluated over an application with cooperation mechanisms. Thus, all the objectives were successful accomplished.

After introducing and presenting the topic of this dissertation as well its objectives and main contributions, chapter two presented some related work on secure m-Health data exchange along with important related work in mobile health as well as some important insights in ubiquitous health and applications.

Chapter three presented the requirement analysis taken before the cryptographic solutions development and integration process. First, essential requirements were defined followed by the usual UML diagrams necessary to model a system, ending with the used technologies.

Chapter four approached the developed cryptographic solutions for mobile health applications in a cooperative environment. Two different approaches were considered and were individually presented and explained in detail. A peer-to-peer messaging forward focusing on assuring protection and privacy of data while being transmitted from mobile node to mobile node or from mobile to/from the WS was considered for DE4MHA approach, where each node encrypts and decrypts messages among them until it reaches the WS. A second approach was considered and developed where each cooperative mobile node acts uniquely as a message forward node, with no content aware of the received and forwarded messages. When the message reaches the WS, it is finally decrypted and verified its authenticity and integrity, encrypting then the message response, being just decrypted when reaching the requester node. This last approach named eC4MHA, has the great advantage of not revealing message content to the cooperative nodes, i.e., besides focusing on the security of the data transmitted among nodes, it also considers the protection and privacy of data received by mobile nodes, presenting as well improved results. Both solutions were developed to assure three fundamental properties, namely data confidentiality, integrity and authenticity.

Chapter five performs the system validation and performance evaluation. After a brief introduction about the used m-Health application (i.e., SapoFit) where the cryptographic mechanisms were integrated, the network scenario for test purposes was presented. Then, experiments were conducted in order to verify the behaviour and efficiency of the system considering a various number of uncooperative mobile nodes, in order to measure the performance of the both developed solutions individually, ending with a comparison between them, concluding that eC4MHA presents an improved performance when compared to DE4MHA.

The cryptographic solutions in this work applied to m-Health applications under a cooperative environment, clearly presents advantages when comparing similar systems without security mechanisms, providing data privacy and protection, not compromising overall network performance. Health data is usually addressed as sensitive data, and may carry information about patients ill history, infectious disease or personal information, which is intended to be private, what requires addressing this thematic with the maximum care. Thus, it is necessary to take into account that due to the advent of mobile health applications, security measures are a fundamental part and should always be carefully addressed.

6.2. Future Work

To conclude this work, it just remains to suggest future research directions based on current work:

- The development of APIs for other mobile platforms, such as iOS from Apple and Windows Phone.
- A classification of sensitive health data addressing different security measures to different levels of sensitiveness.
- A performance assessment study through simulation considering different network scenarios and evaluate the scalability of the proposed solution, may also be considered.

References

[1] S. Akter, J. D'Ambra, and P. Ray, "User Perceived Service Quality of mHealth Services in Developing Countries,", in European Conference on Information Systems (ECIS 2010), Pretoria, South Africa, June 2010.

[2] J. Black, F. Koch, L. Sonenberg, R. Scheepers, A. Khandoker, E. Charry, B. Walker, and N.L. Soe, "Mobile solutions for front-line health workers in developing countries," in IEEE 11th International Conference on e-Health Networking, Applications and Services (*IEEE Healthcom 2009*), Sydney, Australia, December 2009. pp.89-93.

[3] B. Moullec, P. Ray, "Issues in E-Health Cost Impact Assessment," in IFMBE Proceeding of the World Congress on Medical Physics and Biomedical Engineering, Berlin, Germany, Springer Berlin Heidelberg, September 2010, pp. 223–226.

[4] D. Vatsalan, S. Arunatileka, K. Chapman, G. Senaviratne, S. Sudahar, D. Wijetileka, and Y. Wickramasinghe, "Mobile Technologies for Enhancing eHealth Solutions in Developing Countries," in the second International Conference on eHealth, Telemedicine and Social Medicine (ETELEMED 2010), St. Maarten, Netherlands, February 2010, pp.84-89.

[5] R. Makena, C.C. Hayes, “Flexible usage of space for telemedicine,” in IEEE International Conference on Systems, Man, and Cybernetics (IEEE SMC 2011), Anchorage, Alaska, October 2011, pp.1134-1139.

[6] G. Eysenbach, “Medicine 2.0: Social Networking, Collaboration, Participation, Apomediation, and Openness,” Journal of Medical Internet Research, vol. 10, no. 3, 2008.

[7] S. Akter, P. Ray, “mHealth - An Ultimate Platform to Serve the Unserved,” Yearbook of Medical Informatics, Schattauer, Germany, pp.94–100, 2010.

[8] S. Tachakra, X. H. Wang, R. S. H. Istepanian, and Y. H. Song, “Mobile e-Health: The Unwired Evolution of Telemedicine,” Telemedicine Journal and e-Health, vol. 9, no. 3, pp. 247–257, 2003.

[9] S. Laxminarayan, R. S. H. Istepanian, “Unwired E-Med: the next generation of wireless and internet telemedicine systems,” in IEEE Transactions on Information Technology in Biomedicine, vol.4, no.3, pp.189-193, 2000.

[10] R. S. H. Istepanian, and J. C. Lacal, “Emerging mobile communication technologies for health: some imperative notes on m-health,” presented at the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Cancun, Mexico, September 2003, vol. 2, pp. 1414–1416.

[11] R. S. H. Istepanian, S. Laxminarayan, and C. S. Pattichis, “M-Health: Emerging Mobile Health Systems”, 1st ed. Springer, p. 653, 2006.

[12] G. Paré, K. Moqadem, G. Pineau, and C. St-Hilaire, “Clinical Effects of Home Telemonitoring in the Context of Diabetes, Asthma, Heart

Failure and Hypertension: A Systematic Review," Journal of Medical Internet Research, vol. 12, no. 2, 2010.

[13] P. Rubel, J. Fayn, G. Nollo, D. Assanelli, and B. Li, "Toward personal eHealth in cardiology. Results from the EPI-MEDICS telemedicine project." Journal of Electrocardiology, v.38 pp. 100-106, 2005.

[14] C. T. Lin, K. C. Chang, C. L. Lin, C. C. Chiang, S. W. Lu, S. S. Chang, B. S.Lin, H. Y. Liang, R. J. Chen, and Y. T. Lee, "An intelligent telecardiology system using a wearable and wireless ECG to detect atrial fibrillation," IEEE Transactions on Information Technology in Biomedecine, vol. 14, no. 3, pp. 726–733, 2010.

[15] A. Kollmanm, M. Riedl, P. Kastner, G. Schreier, and B. Ludvik, "Feasibility of a Mobile Phone–Based Data Service for Functional Insulin Treatment of Type 1 Diabetes Mellitus Patients," Journal of Medical Internet Research, vol. 9, no. 5, 2007.

[16] S. G. Mougiakakou, et al, "SMARTDIAB: A Communication and Information Technology Approach for the Intelligent Monitoring, Management and Follow-up of Type 1 Diabetes Patients," IEEE Transactions on Information Technology in Biomedicine, vol. 14, no. 3, pp. 622–633, 2010.

[17] F. Zhu, M. Bosch, I. Woo, and S. Y. Kim, "The Use of Mobile Devices in Aiding Dietary Assessment and Evaluation," IEEE journal of Selected Topics in Signal Processing, vol.4, no.4, pp. 756-766,2010.

[18] J. Pollak, G. Gay, S. Byrne, E. Wagner, D. Retelny, and L. Humphreys, "It's Time to Eat! Using Mobile Games to Promote Healthy Eating," IEEE Pervasive Computing, vol.9, no.3, pp.21-27, 2010.

[19] R. Whittaker, E. Dore, D. Bramley,C. Bullen, S. Denny, C.R. Elley, R. Maddison, H. McRobbie, V. Parag, A. Rodgers, and P. Salmon, "A Theory-Based Video Messaging Mobile Phone Intervention for Smoking Cessation: Randomized Controlled Trial", Journal of Medical Internet Research, vol.13, no.1, 2011.

[20] C. Déglise, L. S. Suggs, and P. Odermatt, "Short Message Service (SMS) Applications for Disease Prevention in Developing Countries," Journal of Medical Internet Research, vol. 14, no. 1, p.e3, 2012.

[21] Hammershoj, A. Sapuppo, and R. Tadayoni, "Challenges for mobile application development," IEEE 14th International Conference on Intelligence in Next Generation Networks (ICIN), Berlin, Germany, Oct. 2010, pp.1-8.

[22] G. Kramer, I. Maric, and R.D. Yates, Cooperative Communications, Foundations and Trends in Networking, vol. 1, no. 3-4, pp. 271-425, 2006.

[23] L. Buttyán, and J-P. Hubaux, (2003), "Stimulating Cooperation in Self-Organizing Mobile Ad hoc Networks," Journal of Mobile Networks and Applications, v. 8, no. 5, pp. 579-592, 2003.

[24] M. R. S. Borges, P. Brezillon, J. A. Pino, and J. C. Pomerol, "Bringing context to CSCW," presented at the 8th International Conference on Computer Supported Cooperative Work in Design, 2004, vol. 2, pp. 197–202.

[25] P. Ray, N. Parameswaran, V. Chan, and W. Yu, "Awareness modelling in collaborative mobile e-health," Journal of Telemedicine and Telecare, vol. 14, no. 7, pp. 381–385, Oct. 2008.

[26] V. Chan, P. Ray, and N. Parameswaran, “Mobile e-Health monitoring: an agent-based approach,” Institution of Engineering and Technologies (IET) Communications, vol.2, no.2, pp.223,230, 2008.

[27] B. Silva, J. Rodrigues, I. Lopes, T. Machado, and L. Zhou, “A Novel Cooperation Strategy for Mobile Health Applications,” IEEE Journal on Selected Areas in Communications Special Issue on Emerging Technologies in Communications - eHealth, IEEE Communications Society (in press).

[28] T. Machado, I. Lopes, B. Silva, and J. Rodrigues, “Performance Evaluation of Cooperation Mechanisms for m-Health Applications,” in IEEE Global Communications Conference (GLOBECOM), Anaheim, USA, December 2012, pp. 1664-1669.

[29] Health Level Seven International, “Mobile Health,” [Online]. Available: http://www.hl7.org/Special/committees/mobile/, [Accessed: April, 2013].

[30] K. Malhotra, S. Gardner, and R. Patz, “Implementation of Elliptic-Curve Cryptography on Mobile Healthcare Devices,” in IEEE International Conference on Networking, Sensing and Control, London, UK, April 2007, pp.239-244.

[31] B. Silva, J. Rodrigues, F. Canelo, I. Lopes, and L. Zhou, “A Data Encryption Solution for Mobile Health Apps in Cooperation Environments,” Journal of Medical Internet Research, v. 15, no. 4, 2013.

[32] S. Fox, M. Duggan, “Mobile Health 2012,” [Online]. Available: http://www.pewinternet.org/~/media//Files/Reports/2012/PIP_MobileHealth 2012_FINAL.pdf, [Accessed: April, 2013].

[33] S. Kumar, W. Nilsen, M. Pavel, and M. Srivastava,, “Mobile Health: Revolutionizing Healthcare Through Transdisciplinary Research,” IEE Computer Society , vol.46, no.1, pp.28-35, 2013.

[34] A. Lorenz, and R. Oppermann, “Mobile health monitoring for the elderly: Designing for diversity,” Pervasive and Mobile Computing, vol. 5, no. 5, pp. 478–495, 2009.

[35] M. Weiser, “The Computer for the 21st Century,” IEEE Pervasive Computing, vol. 99, no. 1, pp. 19–25, 2002.

[36] J. Cheng, “Testing and Debugging Persistent Computing Systems: A New Challenge in Ubiquitous Computing,” in IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC 2008), Shanghai, China, December, 2008, vol.1, pp.408-414.

[37] Z. Rashid, U. Farooq, J-K. Jang, and S-H. Park, “Cloud computing aware Ubiquitous Health care system,” in E-Health and Bioengineering Conference (EHB), Lasi, Roumania, November 2011, pp. 1-4.

[38] S. Sano, T. Yoshihisa, and M. Tsukamoto, “Design and Implementation of Device with Alterable Functions for Ubiquitous Computing,” in International Symposium on Ubiquitous Multimedia Computing (UMC 2008), Hobart, Australia, October 2008, pp.226-231.

[39] S. Yoo, S. Jung, J. Choi, and R. Dongwooo, “Development of Ubiquitous Health Monitoring System,” in International Conference on Convergence Information Technology, Gyeongju, South Korea, November 2007, pp.1116-1120.

[40] A. Bourouis, M. Feham, and A. Bouchachia, “A New Architecture of a Ubiquitous Health Monitoring System: A Prototype of Cloud Mobile Health Monitoring System," International Journal of Computer Science Issues (IJCSI 2012), vol. 9, no. 2, 2012.

[41] Y. Jamil, and M. Yuce, “Wireless Body Area Network (WBAN) for Medical Applications”, in New Developments in Biomedical Engineering, Domenico Campolo (Ed.), ISBN: 978-953-7619-57-2, InTech, 2010, pp. 591-598.

[42] C. Lin, R. Lee, and C. Hsiao, “A pervasive health monitoring service system based on ubiquitous network technology,” International Journal of Medical Informatics, vol. 77, no. 7, pp. 461–469, 2008.

[43] I. Brown, and A. A. Adams, “The ethical challenges of ubiquitous healthcare,” International Review of Information Ethics, vol. 8, no. 12, pp. 53–60, 2007.

[44] J. Rodrigues, M. Oliveira, and B. Vaidya, “New Trends on Ubiquitous Mobile Multimedia Applications,” Journal on Wireless Communications and Networking (EURASIP 2010), vol. 2010, no. 1, p. 689517, 2010.

[45] C. Z. Qiang, M. Yamamichi, V. Hausman, D. Altman, and I. Unit, “Mobile Applications for the Health Sector,” [Online]. Available: http://siteresources.worldbank.org/INFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/mHealth_report.pdf, [Accessed: March, 2013].

[46] Google, “Google Android Operating System,” [Online]. Available: http://www.android.com/ [Accessed: February, 2013].

[47] Apple, “Apple iOS,” [Online]. Available: http://www.apple.com/ios/. [Accessed: February, 2013].

[48] Symbian Foundation, “Symbian Operating System,” [Online]. Available: http://licensing.symbian.org/ [Accessed: February, 2013].

[49] Windows. “Windows Phone.” http://www.windowsphone.com/en-us. [Accessed: February 2013].

[50] Google, “Google Play,” [Online]. Available: https://play.google.com/. [Accessed: February, 2013].

[51] Apple, “Apple Store - iTunes,” [Online]. Available: http://itunes.apple.com/. [Accessed: February, 2013].

[52] Nokia, “Ovi Store,” [Online]. Available: http://store.ovi.com/. [Accessed: February, 2013].

[53] Windows. “Windows Phone Store.” http://www.windowsphone.com pt-pt/store. [Accessed February 2013].

[54] Stabilix Corporation, “Stabilix PHR,” [Online]. Available: https://play.google.com/store/apps/details?id=com.stabilix.phr.professional.activity [Accessed: February, 2013].

[55] AimX Labs, “Fast Food Calorie Counter,” [Online]. Available: https://play.google.com/store/apps/details?id=com.concretesoftware.caloriecounter_full [Accessed: February, 2013].

[56] Noom Inc, “CardioTrainer,” [Online]. Available: https://play.google.com/store/apps/details?id=com.wsl.CardioTrainer.pro_feature [Accessed: February, 2013].

[57] Foundation HealthCare Network, “Restaurant Nutrition,” [Online]. Available: https://itunes.apple.com/us/app/restaurant-nutrition/id285180322?mt=8. [Accessed: February, 2013].

[58] Capzure, “Capzule PHR,” [Online]. Available: http://capzule.com/ [Accessed: February, 2013].

[59] PurpleTalk Inc, “Health and Family,” [Online]. Available: http://store.ovi.com/content/100498 [Accessed: February, 2013].

[60] Startlab, “Emergency Kit,” [Online]. Available: http://www.windowsphone.com/en-us/store/app/emergency-kit/ffb4d1ac-5564-48ab-a39d-df694e6c12da [Accessed: February, 2013].

[61] B. Silva, I. Lopes, J. Rodrigues, and P. Ray, “SapoFitness: A mobile health application for dietary evaluation,” presented at the 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services (Healthcom 2011), Columbia, USA, June 2011, pp. 375-380.

[62] E. T. Velde, H. Foeken, and T. Witteman, “Integration of remote monitoring data into the hospital electronic health record system: Implementation based on international standards,” on Computing in Cardiology, Hangzhou, China, September 2011,pp. 581-584.

[63] I. Ćubić, I. Markota, I. Benc, “Application of session initiation protocol in mobile health systems,” presented at the MIPRO 33rd International Convention ,Opatija, Croatia, May 2010, pp.367-371.

[64] B. Kumar, S. P. Singh, and A. Mohan, “Emerging Mobile Communication Technologies for Health,” presented at the International Conference on Computer and Communication Technology (ICCCT 2010), Allahabad, India, September 2010, pp. 828–832.

[65] J. Li, L. Land, and P. Ray, “E-Health readiness framework from Electronic Health Records perspective,” International Journal of Internet and Enterprise Management, vol. 6, no. 4, 2010.

[66] X. Ge, R. F. Paige, and J. A. McDermid, “Domain analysis on an electronic health records system,” presented at the First International Workshop on Feature-Oriented Software Development (FOSD 2009), New York, USA, 2009, pp. 49-54.

[67] “ISO/TR 20514, Health informatics - Electronic health record - Definition, scope and context,” American National Standards Institute (ANSI), 2005, p. 34.

[68] W. Yina, “Application of EHR in Health Care,” on second International Conference on Multimedia and Information Technology (MMIT), Kaifeng, China, April 2010, pp. 60-63.

[69] C. Nosteboom, D. Bastola, and S. Qureshi, “Cycles of Electronic Health Records Adaptation by Physicians: How Do the Positive and Negative Experiences with the EHR System Affect Physicians EHR Adaptation Process?,” Maui, Hawai, USA, January 2012, pp. 1530-1605.

[70] I. Díez, M. Antón-Rodríguez, and F. J. Díaz-Pernas, “Mobile Web Application Development to Access to Psychiatric Electronic Health Records,” Telemedicine Techniques and Applications, Prof. Georgi Graschew (Ed.), ISBN: 978-953-307-354-5, InTech,, 2011, ch.10, pp. 241-257.

[71] D. Patra, S. Ray, and J. Mukhopadhyay, “Achieving e-Health Care in a Distributed EHR System,” in the 11th International Conference on e-Health Networking, Applications and Services (Healthcom 2009), Sydney, Australia, December 2009, pp.101-107.

[72] B. Oladosu, F. A. Ajala, and O. O.Popoola, “On the use of use of Web Services technology in e-health applications,” Journal of Theoretical and Applied Information Technology, 2009.

[73] P. R. Marupally, and V. Paruchuri, “Privacy Preserving Portable Health Record (P^3HR),” in International Conference on Network-Based Information Systems (NBIS 2009), Indianapolis, USA, August 2009, pp. 310-315.

[74] R. Zhang, and L. Liu, “Security Models and Requirements for Healthcare Application Clouds,” in IEEE 3rd International Conference on Cloud Computing (CLOUD), Miami, USA July 2010, pp. 268–275.

[75] HL7, “About HL7,” 2013. [Online]. Available: http://www.hl7.org/about/index.cfm?ref=nav [Accessed: April 2013].

[76] J. Lyman, S. Pelletier, K. Scully, J. Boyd, and J. Dalton, “Applying the HL7 reference information model to a clinical data warehouse,” in IEEE International Conference on Systems, Man and Cybernetics, Washington DC, USA, October 2003, pp.4249-4255.

[77] C. N. Mead, “Data Interchange Standards in Healthcare IT-Computable Semantic Interoperability: Now Possible but Still Difficult. Do We Really Need a Better Mousetrap?,” Journal of Healthcare Information Management, 2006.

[78] R. Sulaiman, D. Sharma, W. Ma, and D. Tran, “A Security Architecture for e-Health Services,” presented at the 10th International Conference on Advanced Communication Technology (ICACT 2008). Gangwon-Do, South Korea, February 2008, pp. 999-1004.

[79] K. Raychaudhuri and P. Ray, “Privacy Challenges in the Use of eHealth Systems for Public Health Management,” International Journal of E-Health and Medical Communications, vol. 1, no. 2, pp. 12–23, 2010.

[80] M. Shanmugam, S. Thiruvengadam, A. Khurat, and I. Maglogiannis, “Enabling Secure Mobile Access for Electronic Health Care Applications,” presented at the Pervasive Health Conference and Workshops, Innsbruck, Austria, December 2006, pp. 1-8.

[81] J. Barnickel, H. Karahan, and U. Meyer, “Security and privacy for mobile electronic health monitoring and recording systems,” in IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM 2010), Montreal, Canada, June 2010, pp. 1-6.

[82] D. Brechlerova and M. Candik, “New trends in security of electronic health documentation,” presented at the 42nd Annual IEEE International Carnahan Conference on Security Technology (ICCST 2008), Prague Czech Republic, October 2008, pp. 13–16.

[83] U. Harish, and R. Ganesan, “Design and development of secured m-healthcare system,” in International Conference on Advances in Engineering, Science and Management (ICAESM 2012) Nagapattinam, India, March 2012, pp. 470–473.

[84] S. Rawat, and G. H. Massiha, “Secure data transmission over wireless networks: issues and challenges,” in IEEE Region 5 Annual Technical Conference, New Orleans, USA, April 2003, pp. 65–68, 2003.

[85] M. Martin, “Everyday Cryptography: Fundamental Principles and Applications”, Oxford University Press Oxford, ISBN: 978-0-19-162588-6, 2012.

[86] A. Boonyarattaphan, Y. Bai, and S. Chung, “A security framework for e-Health service authentication and e-Health data transmission,” in 9th International Symposium on Communications and Information Technology (ISCIT 2009), Icheon, South Korea, September 2009, pp. 1213-1218.

[87] S. Tillich and C. Herbst, “Attacking State-of-the-Art Software Countermeasures—A Case Study for AES,” in the 9th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2008), Washington, USA, August 2008, pp. 228–243.

[88] S. Farah, M. Y. Javed, A. Shamim, and T. Nawaz, “An experimental study on Performance Evaluation of Asymmetric Encryption Algorithms,” presented at the European Conference on Complex Systems (ECCS 2012), Brussels, Belgium, September 2012, pp. 121-124.

[89] W. Diffie, “The first ten years of public-key cryptography,” in Proceedings of the IEEE , May 1988, vol.76, no.5, pp.560-577.

[90] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Communications of the ACM, vol. 21, no. 2, pp. 120–126,1978.

[91] T. Elgamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” in IEEE Transactions on Information Theory, vol. 31, no. 4, 1985.

[92] J. Cochran, "Cryptographic Hash Functions". PhD Dissertation, University of Colorado at Boulder, Colorado, USA, 2008.

[93] R. Rivest, "The MD5 Message-Digest Algorithm," in RFC: 1321, 1992.

[94] Z. Yong-Xia, and Z. Ge "MD5 Research," presented at the 2nd International Conference on Multimedia and Information Technology (MMIT), Kaifeng, China, April 2010, pp. 271-273.

[95] National Institute for Standards and Technology. Secure Hash Standard, April 17 1995.

[96] U.S. Department Of Commerce/ National Institute of Standards and Technology," Digital Signature Standard (DSS)" FIPS PUB 186-2, January 27,2000.

[97] Object Management Group, "UML," [Online]. Available: http://www.uml.org/ [Accessed: February, 2013].

[98] Google, "Android versions distribution," [Online]. Available: http://http://developer.android.com/about/dashboards/index.html [Accessed: May, 2013].

[99] Google, "Android Software Development Kit," [Online]. Available: http://developer .android.com/sdk/index.html [Accessed: April, 2013].

[100] Oracle Corporation, "Java Server Pages," [Online]. Available: http://www.oracle.com/technetwork/java/javaee/jsp/index.html [Accessed: April, 2013].

[101] M. Krishna, and M. Doja, “Symmetric key management and distribution techniques in wireless ad hoc networks,” in International Conference on Computational Intelligence and Communication Networks (CICN), Gwalior, India, October 2011, pp. 727–731.

[102] Bluetooth SIG Inc, “Bluetooth Technical Information,”[Online]. Available: http://www.bluetooth.com [Accessed: May, 2013].

Appendix

This appendix includes the both papers with the main contributions of the work. The first paper is entitled “A Data Encryption Solution for Mobile Health Applications in Cooperative Environments: DE4MHA” [31] and the second was submitted to an international conference (IEEE GLOBECOM 2013) and is entitled “Performance Evaluation of an Enhanced Cryptography Solution for m-Health Applications in Cooperative Environments”.

A Data Encryption Solution for Mobile Health Applications in Cooperation Environments: DE4MHA

Bruno M.C.Silva[1], Joel J. P. C. Rodrigues[1], Fabio Canelo[1], Ivo M. C. Lopes[1], and Liang Zhou[2]
[1] Instituto de Telecomunicações, University of Beira Interior
Rua Marquês d'Ávila e Bolama, 6201-001 Covilhã, Portugal
[2] Nanjing University of Posts and Telecommunications, Nanjing, 210003, China

E-mail: bruno.silva@it.ubi.pt, joeljr@ieee.org, {fabio.canelo, ivo.lopes}@it.ubi.pt, liang.zhou@ieee.org

Abstract

Background: Mobile Health (m-Health) proposes healthcare delivering anytime and anywhere. It aims to answer several emerging problems in health services, including the increasing number of chronic diseases, high costs on national health services, and the need to provide direct access to health services, regardless of time and place. M-Health systems include the use of mobile devices and applications that interact with patients and caretakers. However, mobile devices present several constraints, such as, processor, energy, and storage resource limitations. The constant mobility and often-required Internet connectivity also exposes and compromises the privacy and confidentiality of the Health information.

Objective: This paper aims to present a proposal, construction, performance evaluation, and validation of a data encryption solution for mobile health applications, called DE4MHA, considering a novel and early-proposed cooperation strategy. The goal includes the presentation of a robust solution based on encryption algorithms that guarantee the best confidentiality, integrity, and authenticity of users health information. In this study, we will present, explain, evaluate the performance, and discuss cooperation mechanisms and the proposed encryption solution for mobile Health applications.

Methods: First, we design and deploy the DE4MHA. Then two studies where performed; 1) Study and comparison of symmetric and asymmetric encryption/decryption algorithms in an m-Health application under a cooperation environment; and 2) Performance evaluation of the DE4MHA. Its performance is evaluated through a prototype using an m-Health application for obesity prevention and cares, called SapoFit. We then conduct an evaluation study of the m-Health application with cooperation mechanisms and the DE4MHA using real users and a real cooperation scenario. Along five days, a different group of seven users agree to use and test the SapoFit application using the seven devices available for trials.

Results: Thirty-five users, using SapoFit, participated in this study. The performance evaluation of the application was carried using seven real mobile devices in five different days. The results show that confidentiality and protection of the users health information is guarantied and SapoFit users were able to use with satisfactory quality the m-Health Application. Results also shown the application with the DE4MHA presented nearly the same results as the application without the DE4MHA.

Conclusions: This study shows that DE4MHA offers a robust and reliable health information confidentiality, integrity, and authenticity for mobile health applications. Furthermore, it did not deteriorate the overall performance of the m-Health application maintaining slightly the same performance. Plus, this approach may be used in any health application.

KEYWORDS: Mobile Health; m-Health; Mobile computing; e-Health; Cooperation; Encryption, Security

Introduction

In the last decade health telematics also known as Electronic Health (e-Health), have offered patients that live in remote rural areas, travel constantly, or are physically incapacitated for a given reason, more accessible and affordable healthcare solutions [1,2]. Health telematics are becoming a major improvement in the patient lives, especially those who are disabled, elderly, and chronically ill. Telemedicine assumes the use of medical information, also known as Electronic Health Records (EHRs), exchanged via electronic communications improving the patients' health status [3]. This growing was analogue to the rapidly evolution of information and communication technologies (ICT) infrastructures and rapid access to patient data. The Web 2.0 concept and the emerging Web 3.0 come to offer opportunities to healthcare professionals never given before [4,5]. Now, physicians can perform several tasks through these modern technologies, such as the following:

- Share medical videos (Youtube), photos (Flickr) and presentations (Slideshare)
- Use blogs for posting medical cases and images
- Share hospital management information
- Use social networking to share medical ideas and tasks
- Use RSS feeds to keep track of alerts on their specific interests

With the advent of mobile communications using smart mobile devices that support 3G and 4G mobile networks for data transport, mobile computing has been the main attraction of research and business communities. Thus, offering innumerous opportunities to create efficient mobile health solutions. Mobile health (m-Health) is the new edge on healthcare innovation. It proposes to deliver healthcare anywhere and anytime, surpassing geographical, temporal, and even organizational barriers [6,7]. Laxminarayan and Istepanian defined mobile health for the first time in 2000, as "*unwired e-med*" [8]. In 2003, the term 'm-Health' was defined as: *"emerging mobile communications and network technologies for healthcare systems"* [9]. Laxminarayan et al., in 2006, present a comprehensive study on the impact of mobility on the existing e-Health commercial telemedical systems [10]. Furthermore, it served as basis for future m-health technologies and services [11]. Several research topics related to health have gathered important findings and contributions from m-Health, such as, cardiology [12,13], diabetes [14-16], obesity [17-20], smoking cessation [21], among others. In the above-mentioned medical issues, m-Health applications are applied for health monitoring, diseases prevention and detection, and, in more advanced services, also provide basic diagnosis. M-Health services are also becoming popular in developing countries where healthcare facilities are frequently remote and inaccessible [2,22].

Architectures based on mobile devices and wireless communications present several challenging issues and constraints, such as battery and storage capacity, broadcast constraints, interferences, disconnections, noises, limited bandwidths, and network delays. In this sense, cooperation-based approaches are presented as a solution to solve such limitations, focusing on increasing network connectivity, communication rates, and reliability.

In this paper we present a data encryption solution for mobile health applications (DE4MHA) in cooperative environments guaranteeing data confidentiality, integrity, and authenticity. This novel and early-proposed cooperation strategy [23] for m-Health applications focuses on forwarding and retrieving data to/from nodes that have no direct connection to an m-Health service. In this sense, devices without Internet connectivity can use m-Health applications without problems. This cooperation approach presents a reputation-based strategy where a Web service manages the access control and the cooperation among nodes along with their reputation. It considers the following three main components: a *node control message,* a *requester control message,* and a *cooperative Web service* (CWS). Both control messages are used to manage a local cooperation between two or more nodes. The CWS includes a reputation table for all the nodes and decides which nodes can have access to the requested services. The cooperation strategy and the DE4MHA is deployed and evaluated in an m-Health application for obesity prevention and control, called *SapoFit* [24 - 26]. To the best of our knowledge, there are no cooperative solutions for m-Health services and applications considering this network scenario with constant network disconnection. DE4MHA uses symmetric and asymmetric encryption and decryption techniques. We use the RSA [27] algorithm for asymmetric encryption/decryption to ensure Key exchange confidentiality and the Advanced Encryption Standart (AES) [28] algorithm for symmetric encryption/decryption for data confidentiality. To ensure data integrity we have created message digest that creates a hash of transmitted data and for data authenticity we use a digital signature. We encrypt the hash message with the RSA private Key. To secure the communication with the SapoFit Web Service (WS), we use the HTTPs protocol.

In this paper we report two studies that were performed to design and construct the DE4MHA algorithms: (1) a direct evaluation and comparison of several encryption algorithms and (2) a series of trials evolving 35 persons and seven different mobile devices with SapoFit. The first study revealed what algorithms present the best performance in an m-Health application in cooperation environments. This study evaluates the performance of the DE4MHA over the cooperation mechanisms for m-Health applications.

Methods

This study used an available m-Health application, called SapoFit to deploy, evaluate, and validate the proposed solution. This application uses a cooperation strategy that addresses two related limitations to m-Health applications with service-oriented architectures, namely the network infrastructure and Internet connectivity dependency. It follows a reputation-based approach as an incentive method for cooperation, which includes a Web service to manage all the network cooperation. It is responsible for verifying the cooperation status of neighbor nodes and to provide relay nodes the required data in order to perform a full data request.

Cooperation Strategy for m-Health applications

The cooperation strategy for m-Health applications with service oriented architectures (SOAs) is based on the following two mobile modules and one remote module: i) the *node control message,* ii) the *requester control message*, and iii) the *cooperative Web service* (CWS).

The mobile *nodes control messages* aim to provide an awareness of the relay node status, i.e., if the node is willing to cooperate and in what conditions. It contains the established node unique identifier, the battery state, the Internet connectivity status, and the cooperation status (i.e., if it is cooperative or not).

The *requester control message* is sent by the initial requester node first (the mobile device with m-health application requesting health data), and it comprises the following five main components: 1) the requester ID, the node unique identifier; 2) the service request, i.e., what the node is specifically requesting (e.g., the login token or its health profile); 3) the neighbors list; 4) the reputation list; and 5) the achieved cooperation time (ACT).

The *cooperative Web service* (*CWS*) is responsible for performing a fair access control to data. Thus, according to the received reputation information, the Web service holds the final reputation list in order to decide if a requester node should have access to the m-Health application Web service or not. The reputation list contains all registered network nodes with their identifier and their corresponding reputation value.

Figure 1 presents a user scenario of the m-Health cooperation approach. *User A* has network connectivity and cooperates, the status value is according to the battery status. *User B* has network connectivity and does not cooperate. Then, the status value will suffer a negative impact according to the battery status. *Users C* and *D* do not have network connectivity. *User C* queries *User A* for cooperation and receives a positive response and all the requested data. *User D* queries *User B* for cooperation and receives a negative response. Then, *User D* requests data from *User C* that answers this request, getting positive status by cooperating.

Cooperating nodes have a better reputation, and have priority over selfish nodes to access the m-Health application services.

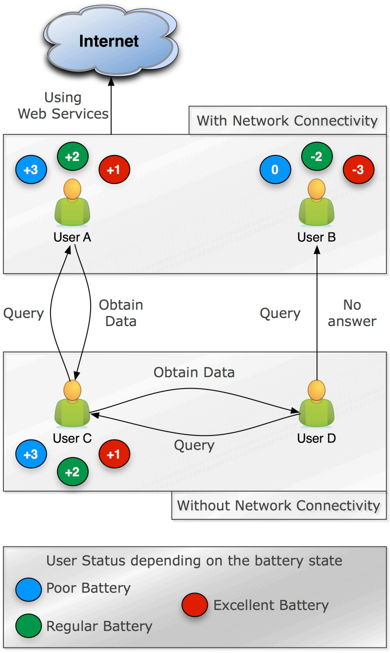
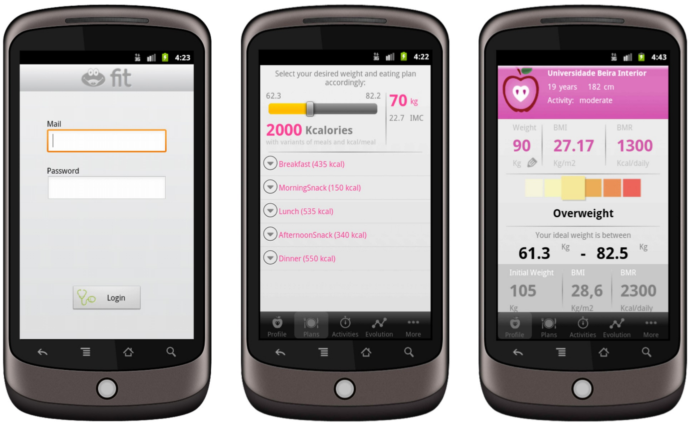


Fig 1. Illustration of the interaction for an m-Health application with the proposed cooperation approach for 4 users.

SapoFit Application

SapoFit is a weight control mobile application that allows users to keep track of weight in a healthier and more practical way. SapoFit allows users to control their weight, body mass index (BMI), basal metabolic rate (BMR), sports activity, and the possibility to follow food plans based on their needed calories. In this m-Health application all the users must be registered in a Web service. Figure 2 presents the following three main activities screenshots of SapoFit application: *Login, Plans,* and *User Profile.*



Select your desired weight and eating plan accordingly:

62.3 82.2 70 kg 22.7 IMC

2000 Kcalories
with variants of meals and kcal/meal

Breakfast (435 kcal)
MorningSnack (150 kcal)
Lunch (535 kcal)
AfternoonSnack (340 kcal)
Dinner (550 kcal)

Universidade Beira Interior
19 years 182 cm
Activity: moderate

Weight	BMI	BMR
90	27.17	1300
Kg	Kg/m2	Kcal/daily

Overweight

Your ideal weight is between
61.3 Kg - 82.5 Kg

Initial Weight	BMI	BMR
105	28,6	2300
Kg	Kg/m2	Kcal/daily

Fig 2. Three main activities screenshots of SapoFit application: *Login, Plans,* and *User Profile.*

Data Encryption Algorithm for Mobile Health applications (DE4MHA)

The process begins with a mobile node (a person using SapoFit) trying to access the SapoFit Web Service that contains the user profile, weight measures, fitness, and diet indications.

A SapoFit user (mobile requester node) without network connectivity and therefore without access to the SapoFit Web services (WS) obtains the required health information through cooperation. Another SapoFit user with network connectivity (mobile requested node) will forward the requested health information from the SapoFit Web service. Both the requested and requester nodes will create a pair of RSA keys and send to both requester and requester node their public keys (through Bluetooth). After the public key exchange, the requested node creates an AES session key.

The next step is the creation of the digest message and its encryption using the private key. The MD5 algorithm was used to create a 128 bits hash. For data authenticity we use digital signature. A digital signature is created for the message containing requested health information. This digital signature allows any node to verify that message is the original one. By decrypting the digital signature with the public key, the original digest message is obtained. The receiver node then creates a new hash of the received message and compares it to the decrypted digest message to guarantee authenticity. The digital signature is then added to the message. When the message containing the session key is received, if its integrity and authenticity is verified, the requester node then sends an acknowledgement (*ack*) to the requested node. This method guaranties safe communication between nodes, otherwise if the integrity and authenticity is not verified the communication between nodes is ended.

A mobile node with network connectivity will access the cooperative WS to obtain the required health information. To secure all communication with the WS the Secure Socket Layer (SSL) over the HTTP (also known as HTTPs) is used. Therefore, it grants confidentiality, integrity, and authenticity of all retrieved health data from the Web service.

Two studies were performed. 1) a study evaluating what symmetric and asymmetric algorithm presents the best performance in an m-Health application in cooperation environment, and 2) a series of trials evolving 35 persons and seven different mobile devices with SapoFit. This study evaluates the performance of the DE4MHA over the cooperation mechanisms.

Study 1: Study and comparison of symmetric and asymmetric encryption/decryption algorithms in an m-Health application under a cooperation environment

Symmetric Algorithm

In order to choose the best suited symmetric encryption algorithm for SapoFit application (DE4MHA), performance experiments were conducted using four different encryption algorithms, namely AES, Triple Data Encryption Standard

(3DES) [29], RC4 [30], and Blowfish [31], using the data size to encrypt as a performance metric.

Asymmetric Algorithm

Concerning the choice of an asymmetric algorithm in order to exchange session keys between mobile nodes, two options were considered. We tested RSA, which enables encrypting the session key, subsequently being sent, and Diffie-Hellman [32] which allows users to share a secret, generating then a session key based on the shared secret. For our network scenario these are the most suited algorithms. Other encryption algorithms were studied, such as the Elliptic Curve Cryptography (ECC) algorithm [33].

Study 2: Performance evaluation of the DE4MHA

The performance evaluation study was carried using seven real mobile devices, which have been used seven times in five different days with a total of 35 different users who tested successfully the application. Figure 3 presents the seven different mobile devices with different hardware and software used with the SapoFit m-Health application.

Cooperative nodes, without network connection, cooperate with each other through Bluetooth. The communication with the CWS can be obtained through the device Wi-Fi or Edge/3.5G/4G modules. The CWS was developed with the help of Java Server Pages (JSP) technology, using the REST architecture. To serve the Web Service the Apache Tomcat Web Server is used.

Non-cooperative cases where controlled and measured to a maximum of 4 to guarantee the minimum service performance. Through cooperation all the devices can indeed use the m-Health application. However, uncooperative nodes affect directly the service delivery probability, service average delay, and the overall network performance. Performance metrics considered in this study are the service delivery probability (in percentage) and the service average delay (in seconds). We present a comparison of the performance of the m-Health application with and without the DE4MHA.

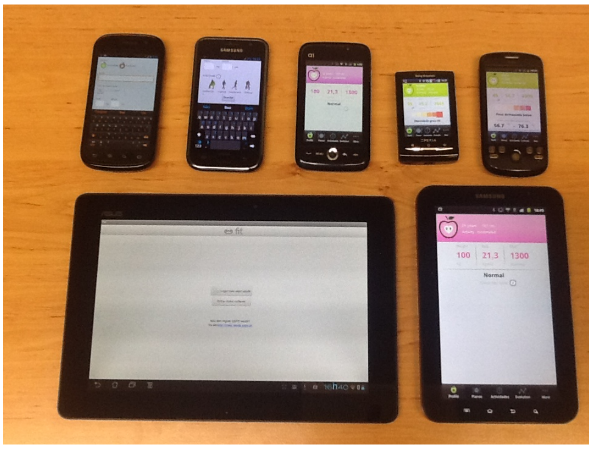


Fig. 3. Mobile devices used for trials with the SapoFit m-Health application.

User Trials Evaluation of DE4MHA in Cooperative Environments

User trials were conducted within the University informatics department using seven devices available for trials. Along five days, a different group of seven students agree to use and test the SapoFit application. Users were in constant movement moving far away from each other. This mobility is necessary to test the network scenario forcing network delays and disconnections. The cooperative strategy and the DE4MHA is ubiquitous to its user and through out the trials users only experience and use the obesity prevention services that SapoFit offers without any constraints or perception of any cooperation mechanism or encryption algorithm that is embedded in the m-Health application.

While conducting the experiments, almost every users asked if their information was being kept secure or not, clearly showing that they did not wanted their health information to be available or disclosed to unauthorized people, revealing privacy concerns. Another frequent raised question concerns the need to share Internet connectivity to other users.

We explain and justify that sharing and cooperating with other users is essential to obtain a better reputation. Furthermore we demonstrate to them that SapoFit is no intrusive with other user personal data on the mobile device and only requests SapoFit services.

After the experiments, the users completed a survey evaluating their experience. The questions are listed in Table I and the results may be seen in Figure 4. As can be observed, the results are very good the received feedback is very promised for this solution.

Table I. Survey Questions.

Question	Description
Q1	Without network connectivity, the user always gets the required information?
Q2	Without network connectivity, the required information was delivered in a confortable time?
Q3	Understanding the implemented cooperation strategy and its benefits, are you willing to cooperate and share the device/network resources with other users?
Q4	With the encryption strategy applied to SapoFit, do you trust that your personal health information is secure?
Q5	Was the mobile device affected by the application cooperation and encryptions mechanisms (broadband, battery, etc.)?

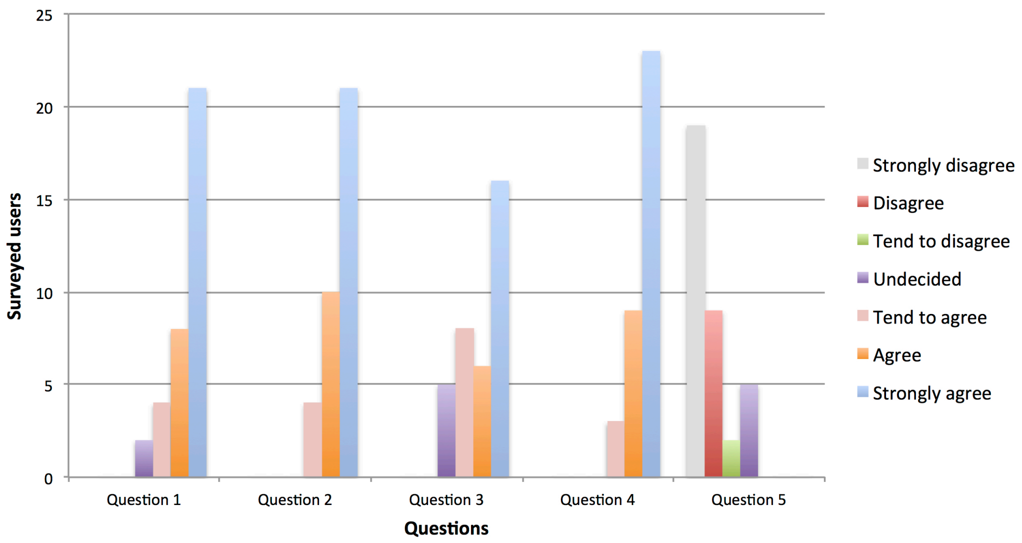


Fig. 4. Results of the survey evaluating the main questions about the performance of the m-Health application with the proposed cooperation strategy and encryption solution.

Results

Symmetric Algorithm

As may be seen in Figure 5, results shown that when data size to encrypt grows, the encryption time (seconds) also increases, as expected. When comparing small amounts of data, all the four algorithms present similar results. However, AES algorithm presents better results since the encryption time of bigger data tends to grow up very slowly. The other three experimented algorithms all tend to grow up exponentially as data size to encrypt overcomes 1000KB. The 3DES algorithm presented the maximum observed encryption time, encrypting 10000KB of data, which took on average 14.3 seconds. With the same amount of data the AES encryption time was only 0.0045 seconds. Regarding decryption we obtained nearly the same results. AES algorithm decryption time is in average 0.0038 seconds to decrypt 10000KB of data.

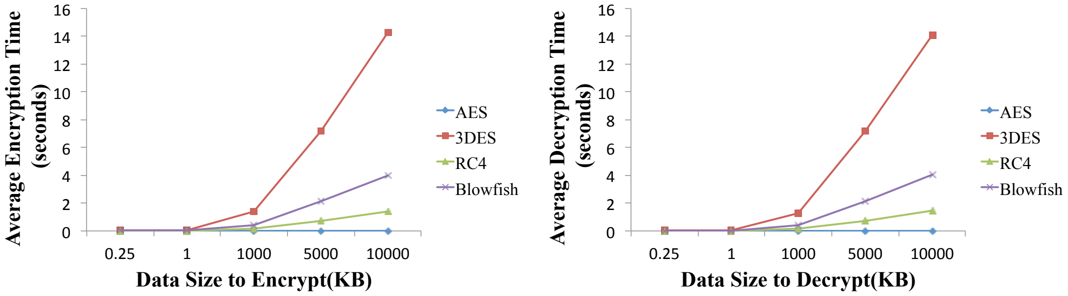


Fig. 5. Comparison of Encryption and Decryption of Symmetric algorithms (AES, 3DES, RC4, and Blowfish).

DE4MHA aims mobile health applications in a cooperative environment. Therefore, the amount and size of data exchange in these network scenarios is unknown and unpredictable. Through the obtained results (Figure 5) we concluded that the AES algorithm with a 128 bits key encryption is the most efficient algorithm for these network scenarios, when handling with both small and large amounts of data.

Asymmetric Algorithm

Regarding the choice of an asymmetric algorithm in order to exchange session keys between mobile nodes, two options were considered, the RSA and the Diffie-Hellman algorithms. The RSA encrypts the session key, subsequently being sent, and Diffie-Hellman allows users to share a secret, generating then a session key based on the shared secret.

Several experiments were performed with both algorithms with RSA presenting better encryption times than Diffie-Hellman, due to the high amount of computation needed by Diffie-Hellman and the low processing capacity of mobile devices.

DE4MHA Performance evaluation results

In the presented scenario, all the devices have Bluetooth class 2 modules, but only three devices have Internet connectivity. Users without Internet connectivity must use the integrated cooperation mechanisms in order to obtain the requested health information. When the number of uncooperative nodes increases, the service delivery probability decreases. The service average delay also presents the same behavior, as expected. Increasing the number of uncooperative nodes the service average delay increases.

Figure 6 shows results of the service delivery probability and the service average delay in function of the number of uncooperative mobile nodes with and without the DE4MHA. As may be seen, the probability that a request is successfully answered in function of uncooperative nodes in the network decreases with the increasing of uncooperative mobile nodes. Taking into account both approaches, with and without DE4MHA, it is observed that DE4MHA presents a slightly worse result. The service average delay also grows when the number of uncooperative mobile nodes increases, as expected. The results of the DE4MHA are also a slightly worse but practically insignificant.

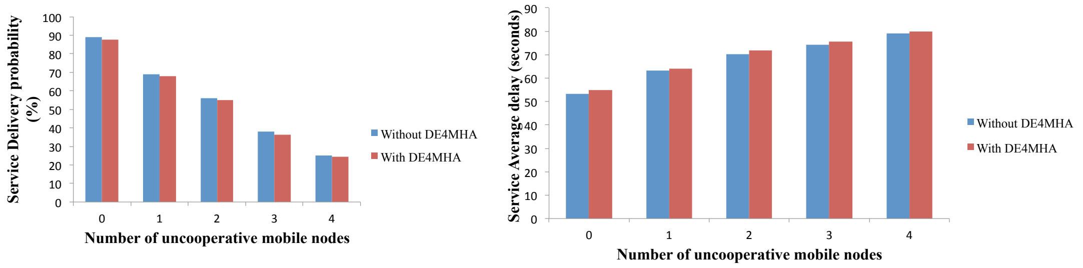


Fig. 6. Service delivery probability and service average delay in function of the number of uncooperative mobile nodes with and without the DE4MHA.

Discussion

Our main goal was focused on the proposal and construction of a security encryption/decryption based solution in a cooperative environment for m-health applications. We aimed to ensure data confidentiality, integrity, and authenticity. Privacy is a top priority issue in m-Health services and applications that deal with user sensitive information. On m-Health applications several security issues must be considered, such as personal information management, secondary use of personal information, improper use of personal information, and errors with stored personal information. Therefore, cryptographic mechanisms can be seen as a solution to guarantied data confidentiality and protection [34].

In a mobility and cooperative environment with constant health data forward and retrieval, studying and developing security mechanisms become crucial. Several experiments were conducted, involving 35 different users, in order to check if they could distinguish the application running with and without the DE4MHA embedded. Through the trials we concluded that users could not tell which application had the DE4MHA embedded mainly because the time response taken to obtain the user health information being nearly the same as the one without DE4MHA. The DE4MHA is implemented in a ubiquitous manner so users would be able to keep using the application without noticing changes or any privacy mechanisms.

All along we had to lead with several limitations. The main limitation concerned applying security on mobile devices due to the low processor capacity when compared with traditional PCs, though nowadays we are seeing a tremendous improvement on this matter, with a few devices being capable to compete with the traditional PCs. Due to this, we experimented several security algorithms concerning confidentiality (AES, RC4, 3DES and Blowfish), integrity (MD5 and SHA1), and authenticity (RSA with MD5 and DSA with SHA1) in order to verify which one had a better performance in a mobile environment.

During the experiments some users without Internet connectivity who wanted to obtain health information, were in constant movement moving far away from other users with cooperation mechanism embedded, resulting in a failure obtaining the desired health information due to not being in a range of 10 meters that Bluetooth class 2 modules require. Another limitation, though not related to security, regards the number of uncooperative nodes (mobile nodes that may not want to cooperate or they may not have cooperation mechanisms embedded), compromising service response probability.

Conclusion

This paper proposed a data encryption solution for mobile health applications, called DE4MHA. The data encryption algorithm DE4MHA with cooperation mechanisms in mobile health allow users to safely obtain health information with the data being carried securely. These security mechanisms did not deteriorate the overall network performance and the application, maintaining slightly the same performance. However, it offers a robust and reliable increase of privacy, confidentiality, integrity, and authenticity of their health information. Although it was experimented on a specific m-Health application, called SapoFit, both DE4MHA and the cooperation strategy can be deployed in a given m-health application.

Acknowledgments

This study has been partially supported by *Instituto de Telecomunicacões,* Next Generation Networks and Applications Group (NetGNA), Portugal, by National Funding from the FCT – *Fundacão para a Ciência e a Tecnologia* through the PEst-OE/EEI/LA0008/2011 Project, by National Natural Science Foundation of China (Grant No. 61201165 and No. 61271240), and by the AAL4ALL (Ambient Assisted Living for All) project co-funded by COMPETE under FEDER via QREN Programme.

References

1. Moullee BL, Ray P. Issues in E-Health Cost Impact Assessment. IFMBE Proceeding of the World Congress on Medical Physics and Biomedical Engineering. Munich, Germany. 2009 September 7-12. 223-226. doi: 10.1007/978-3-642-03893-8_63.

2. Akter S, D'Ambra J, Ray P. User Perceived Service Quality of mHealth Services in Developing Countries. European Conference on Information Systems. Pretoria, South Africa. 2010 June 6-9.

3. United Nations Foundation, Vodafone Group Foundation, and Telemedicine Society of India. mHealth and Mobile Telemedicine - an Overview. 2008 July 27-August 1.

4. Subramoniam S, Saifullah SAHM. Healthcare 2.0. IT Professional. 2010 Nov-Dec; 12(6): 46-51.

5. epSOS – the European eHealth Project. URL:http://www.epsos.eu/. [Accessed: 2013-01-28]. (Archived by WebCite® at http://www.webcitation.org/6E0ipZcb2).

6. Akter S, Ray P. mHealth - an Ultimate Platform to Serve the Unserved. Year Med Inform. 2010:94–100. PMID:20938579.

7. Tachakra S, Wang XH, Istepanian RS, Song YH. Mobile e-health: the unwired evolution of telemedicine. Telemed J E Health. 2003; 9: 247–257. PMID:14611692.

8. Istepanian RSH, Laxminaryan S. UNWIRED, the next generation of wireless and internet able telemedicine systems-editorial paper. IEEE Transactions on Information Technology in Biomedicine.2000; 4:189–194. PMID:11026588.

9. Istepanian RSH, Lacal JC. Emerging mobile communication technologies for health: some imperative notes on m-health. Engineering in Medicine and Biology

Society. *2003.* Proceedings of the 25th Annual International Conference of the IEEE. 2003 September 17-21; 2:1414-1416.doi: 10.1109/IEMBS.2003.1279581.

10. Istepanian RSH, Laxminarayan S, Pattichis, CS. M-Health: Emerging Mobile Health Systems. Springer, NY. 2006. ISBN 978-0-387-26559-9.

11. Pare G, Moqadem K, Pineau G, St-Hilaire C. Clinical effects of home telemonitoring in the context of diabetes, asthma, heart failure and hypertension: a systematic review. J Med Internet Res.2010;12(2):e21. doi: 10.2196/jmir.1357.

12. Fayn J, Rubel P. Towards a personal health society in cardiology. IEEE Trans Inf Technol Biomed. 2010;14(2):401–409. PMID:20007033.

13. Lin CT, Chang KC, Lin CL, Chiang CC, Lu SW, Chang SS, Lin BS, Liang HY, Chen RJ, Lee YT, Ko LW. An intelligent telecardiology system using a wearable and wireless ECG to detect atrial fibrillation. IEEE Trans Inf Technol Biomed. 2010 May;14(3):726-733. PMID: 20371411.

14. Kollmann A, Riedl M, Kastner P, Schreier G, Ludvik B. Feasibility of a mobile phone-based data service for functional insulin treatment of type 1 diabetes mellitus patients. J Med Internet Res. 2007 Dec 31;9(5):e36. doi: 10.2196/jmir.9.5.e36.

15. Mougiakakou SG, Bartsocas CS, Bozas E, Chaniotakis N, Iliopoulou D, Kouris I, Pavlopoulos S, Prountzou A, Skevofilakas M, Tsoukalis A, Varotsis K, Vazeou A, Zarkogianni K, Nikita KS. SMARTDIAB: a communication and information technology approach for the intelligent monitoring, management and follow-up of type 1 diabetes patients. IEEE Trans Inf Technol Biomed. 2010 May;14(3):622-33. PMID: 20123578.

16. Jara AJ, Zamora MA, Skarmeta AFG. An Internet of things-based personal device for diabetes therapy management in ambient assisted living (AAL). Personal and Ubiquitous Computing. April 2011; 15(4):431-440.

17. Zhu F, Bosch M, Woo I, Kim S, Boushey CJ, Ebert DS, Delp EJ. The Use of Mobile Devices in Aiding Dietary Assessment and Evaluation. IEEE J Sel Top Signal Process. 2010 Aug;4(4):756-766. PMID: 20862266.

18. Pollak J, Gay G, Byrne S, Wagner E, Retelny D, Humphreys L. It's Time to Eat! Using Mobile Games to Promote Healthy Eating. Pervasive Computing, IEEE. 2010 July-Sept; 9(3):21-27. doi: 10.1109/MPRV.2010.41.

19. Patrick K, Raab F, Adams MA, Dillon L, Zabinski M, Rock CL, Griswold WG, Norman GJ. A text message-based intervention for weight loss: randomized controlled trial. J Med Internet Res. 2009 Jan 13;11(1):e1. PMID: 19141433.

20. Watson A, Bickmore T, Cange A, Kulshreshtha A, Kvedar J. An internet-based virtual coach to promote physical activity adherence in overweight adults:

randomized controlled trial. J Med Internet Res. 2012 Jan 26;14(1):e1. PMID: 22281837.

21. Whittaker R, Dorey E, Bramley D, Bullen C, Denny S, Elley CR, Maddison R, McRobbie H, Parag V, Rodgers A, Salmon P. A theory-based video messaging mobile phone intervention for smoking cessation: randomized controlled trial. J Med Internet Res. 2011 Jan 21;13(1):e10. PMID: 21371991.

22. Déglise C, Suggs LS, Odermatt P. Short message service (SMS) applications for disease prevention in developing countries. J Med Internet Res. 2012 Jan 12;14(1):e3. PMID: 22262730.

23. Silva BMC, Rodrigues JJPC, Lopes IMC, Machado TMF, Zhou L. A Novel Cooperation Strategy for Mobile Health Applications. IEEE Journal on Selected Areas in Communications Special Issue on Emerging Technologies in Communications - eHealth, IEEE Communications Society (in press).

24. Silva BMC, Lopes IMC, Rodrigues JJPC, Ray P. SapoFitness: A mobile health application for dietary evaluation. 13th IEEE International Conference on e-Health Networking Applications and Services (IEEE HEALTHCOM 2011). Columbia, MO, USA. 2011 June 13-15. doi: 10.1109/HEALTH.2011.6026782.

25. Rodrigues JJPC, Lopes IMC, Silva BMC, Torre ID. A new mobile ubiquitous computing application to control obesity: SapoFit. Inform Health Soc Care. 2012 Jun 1. [Epub ahead of print] PMID: 22657250.

26. SapoFit. URL:http://itunes.apple.com/pt/app/sapo-fit/id438487775?mt=8. [Accessed: 2012-12-15] (Archived by WebCite® at http://www.webcitation.org/6Cw2BHsOA).

27. Jonsson J and Kaliski B. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. URL:http://www.rfc-editor.org/. [Accessed: 2012-12-15] (Archived by WebCite® at http://www.webcitation.org/6Cw66XuiI).

28. Raeburn K. Advanced Encryption Standard (AES) Encryption for Kerberos 5. URL:http://www.rfc-editor.org/. [Accessed: 2012-12-15] (Archived by WebCite® at http://www.webcitation.org/6Cw4IKbXi).

29. Housley R. Triple-DES and RC2 Key Wrapping. URL: http://www.rfc-editor.org/. [Accessed: 2012-12-15] (Archived by WebCite® at http://www.webcitation.org/6Cw4ZXBdH).

30. Jaganathan K, Zhu L, Brezak J. The RC4-HMAC Kerberos Encryption Types. URL:http://www.rfc-editor.org/. [Accessed: 2012-12-15] (Archived by WebCite® at http://www.webcitation.org/6Cw5Lwx1B).

31. Shirey R. Internet Security Glossary, Version 2. URL: http://www.rfc-editor.org/. [Accessed: 2012-12-15] (Archived by WebCite® at http://www.webcitation.org/6Cw5pWnxS).

32. Rescorla E. Diffie-Hellman Key Agreement Method. URL:http://www.rfc-editor.org/. [Accessed: 2012-12-15] (Archived by WebCite® at http://www.webcitation.org/6Cw6I1jk5).

33. McGrew D, Igoe M, Salter M. Fundamental Elliptic Curve Cryptography Algorithms. URL:http://www.rfc-editor.org/rfc/rfc6090.txt. [Accessed: 2013-01-28] (Archived by WebCite® at http://www.webcitation.org/6E0ktAxqb).

34. Raychaudhuri K, and Ray P. Privacy Challenges in the Use of eHealth Systems for Public Health Management. International Journal of e-Health and Medical Communications, IGI-Global. 2010;1(2): 12–23. doi:10.40.18/jehmc.2010040102.

Performance Evaluation of an Enhanced Criptography Solution for m-Health Applications in Cooperative Environments

Fabio Canelo[1], Bruno M.C. Silva[1], Joel J.P.C. Rodrigues[1], and Zuqing Zhu[2]

[1] Instituto de Telecomunicações, University of Beira Interior, Covilhã, Portugal
[2] School of Information Science and Technology, University of Science and Technology of China, Hefei, China

fabio.canelo@it.ubi.pt; bruno.silva@it.ubi.pt; joeljr@ieee.org; zqzhu@ieee.org

Abstract— **Mobile health (m-Health) applications delivers healthcare services through mobile applications regardless of time and place. An m-Health application makes use of wireless communications to sustain its health services and often providing a patient-doctor interaction. Therefore, m-Health applications present several challenging issues and constraints, such as, mobile devices battery and storage capacity, broadcast constraints, interferences, disconnections, noises, limited bandwidths, network delays, and of most importance, privacy and confidentiality concerns. This paper proposes a novel and enhanced cryptography solution in a cooperative environment considering a novel and early-proposed cooperation strategy for m-Health Applications. This proposal aims to face the challenges related to privacy and security issues of all forwarded and retrieved data concerning user sensitive information. Furthermore, it presents a performance evaluation of this proposal considering a comparison with an earlier proposed encryption strategy for the same cooperative environment.**

Keywords— Mobile Health; m-Health; Mobile computing; e-Health; Cooperation; Cryptography

Introduction

M-Health is considered the future of health telematics and a central point on healthcare innovation. It can be defined as the integration and application of health services in mobile technologies intended to deliver healthcare anywhere and anytime. Therefore, offering more ease of access to healthcare solutions overcoming issues like geographical, temporal, and even organizational barriers [1-2]. Hence, m-Health is commonly used in telemedicine allowing e.g., personal health care remote management and patient's health status monitoring [3]. Mobile devices and wireless communications support typical m-Health applications. However, these applications present several challenging issues and constraints, such as, battery and storage capacity, broadcast constraints, interferences, disconnections, noises, limited bandwidths, and network delays. Cooperation-based approaches are presented as a solution to solve such limitations and to improve wireless networks performance [4]. In the absence of a stable network infrastructure, mobile nodes cooperate with each other performing all networking functionalities [5].

A novel and early proposal of a reputation-based cooperation strategy for m-Health services, was presented in [6]. The main goal of this proposal allows and delivers access to health data despite connectivity state and availability. However, cooperation among mobile devices involves sensitive and private health data exchange, like personal health records or health treatment plans that are desirable to be kept private and undisclosed to unauthorized people. Health data privacy, integrity and authentication are major concerns when using m-Health applications. Cryptography algorithms are presented has a solution to the above mentioned security concerns. Due to the advent and evolution of current mobile devices, cryptographic algorithms are now capable of securing and exchanging data without the concern of mobile resources that could decrease cooperative gains and compromising the overall efficiency and effectiveness of the network or even degrading the mobile application user experience.

This paper presents a novel and enhanced cryptography strategy for m-Health applications in a cooperative environment called Enhanced Cryptography for Mobile Health Applications (eC4MHA). It focuses on assuring and guarantying the m-Health application data confidentiality, integrity, and authenticity. The performance assessment and evaluation of the proposal considers a comparison to a previous and early-proposed proposed encryption strategy for m-Health applications, called DE4MHA [7]. This evaluation studies the impact of the cryptography strategy on the performance of an m-Health application under the cooperative solution and environment. The evaluation was conducted using an m-Health application, named SapoFit, that aims obesity prevention and control [8-10].

The remainder of this paper is organized as follows. Section II elaborates on related work regarding health data privacy and security in a mobile environment that contributes to the proposed cryptography solution. Section III describes the proposed m-Health cryptography strategy in a cooperative environment while a performance evaluation and validation through a real m-Health application is presented in Section IV. Section V concludes the paper and points out further research points.

Related Work

Security is expected to be a central point in the evolution of pervasive m-Health applications towards mobile wireless networks. Energy saving in a mobile environment is a major concern that must be addressed carefully due to mobile devices limited resources. Often, typical m-Health network architectures require connectivity availability to operate with Web Services (WSs). This interaction is responsible for major energy consuming. Wi-Fi and Bluetooth transmissions are responsible for a significant consumption of battery power, specially Wi-Fi that can achieve up to 50% of the total energy unlikely Bluetooth which is believed to consume less than 10% battery power [11]. Furthermore, the mobile devices processing capability must be considered while developing mobile applications.

Cryptography algorithms are solutions to guarantee data confidentiality, integrity, and authenticity [12]. The use of these algorithms in mobile and wireless communications, represent time consuming and costly tasks to be executed. Therefore, a lightweight rather than complex approach is desired in such context. Securing e-Health data in a mobile environment has been a matter with high importance, mainly due to the data sensitivity associated exchanged between users [13]. In [14], it is proposed an architecture that allows exchanging patient's medical record in a secure way through existing infrastructure of mobile operators. Generic Bootstrapping Architecture (GBA) is used to enable user authentication while the other entity in the communication (service provider, hospital, and network operator) authenticates through usage of Public Key Infrastructure (PKI). To guarantee a secure communication, encryption and digital signature techniques are used. In [15], authors describe a new trend in security of e-health data presenting XML security solutions describing some selected solutions in health data. eXtensible Access Control Markup Language (XACML) and Security Assertion Markup Language (SAML) are presented enabling authentication and authorization in a large network space. Moreover, SAML enables transmission of authentication data between parties, namely between an identity provider and a service provider. XACML defines access control policies and a processing model describing how to evaluate authorization requests according to the rules defined in the policies.

The above-mentioned approaches present features required in an m-health scenario. However, some limitations arise, specifically the first one is the mobile operator dependency and the second one is focused towards systems exchanging data in XML format. Furthermore, cooperative scenarios present its own specific features and limitations, such as node misbehaviour or loss of connections requiring special care. Hence, an early-proposed encryption strategy for such cooperative scenarios was proposed in [7], called DE4MHA. This proposal addresses data privacy and protection achieved through a hybrid approach using both symmetric and asymmetric cryptography, not being confined to a specific mobile operator or a specific data file format. DE4MHA allows data exchange among nodes assuring data confidentiality through a symmetric algorithm, namely Advanced Encryption Standard (AES). An integrity and authenticity mechanism is achieved through usage of a combination of the Message Digest 5 (MD5) algorithm and the asymmetric algorithm Rivest, Shamir, Adleman (RSA). Afterwards, an output called message digest is calculated from the original message to be sent and then encrypted with RSA's private key. The result of the last operation (digital signature) is appended to the message, providing to the receiver the possibility of confirming if the received data is the original one and that it was sent from the expected source. This approach considers a peer-to-peer node-forwarding scheme based on node reputation, with message content aware, limiting WS access to nodes with low reputation value.

The cryptography strategy proposed in this paper overcomes the above-mentioned limitation that includes nodes forwarding messages with no content-aware other than strictly required information. Furthermore, mobile nodes act merely as messages forwarders. They do not perform encryption tasks, increasing the overall network performance in comparison to DE4MHA (demonstrated in section IV).

Cryptography Solution for m-Health Applications in Cooperative Environments

This section presents the reputation-based cooperation strategy for m-Health applications and the cooperative environment. Furthermore, it describes in detail, the novel cryptography solution for cooperative m-Health applications (eC4MHA).

A. Cooperation mechanisms

This reputation-based cooperation strategy relies on a WS to manage a fair access control to data and cooperation among nodes based on their reputation. According to the received reputation information, the WS decides if a requester node should have access to the requested data or not. Cooperating nodes with better reputation have priority over selfish nodes to access the m-Health application services.

This cooperation strategy for m-Health applications with service oriented architectures (SOAs) is based on two mobile and a remote module: *i*) the *node control message, ii*) the *requester control message*, and *iii*) the *cooperative Web service* (CWS).

The *node control messages* provide an awareness of the node status, i.e., if the node is willing to cooperate and in what conditions. It includes the node unique identifier, battery state, Internet connectivity status, as well the node cooperation status. The *requester control message* is first sent from the requester node (a mobile node without Internet connection and therefore without access to the m-Health application services) and it contains five main components: 1) the requester ID, the node unique identifier; 2) the service request, i.e., what the node is specifically requesting (e.g., the login token or its health profile); 3) the neighbors list; 4) the reputation list; and 5) the achieved cooperation time (ACT).

The *cooperative Web service* (*CWS*) is responsible for performing a fair access control to data, deciding if a node should be able to get the requested data or not. Thus, according to the received reputation information, the *CWS* holds the final reputation list in order to decide if a requester node should have access to the m-Health application Web service or not. The reputation list contains all the registered network nodes with their identifier and their respective reputation value.

B. *Enhanced Cryptography Solution for M-Health Applications: eC4MHA*

eC4MHA focuses on three major concerns on mobile and wireless communications, namely data confidentiality, integrity, and authenticity. Confidentiality assures that data is not made available or disclosed to unauthorized persons. However, guarantying data confidentiality may not be enough to ensure overall security and privacy of personal health information. Data integrity and authenticity assures that data has not been modified and its source is reliable.

Assuring Data Confidentiality

Two approaches were considered, 1) using only asymmetric cryptography, and 2) a hybrid approach using both asymmetric and symmetric cryptography. The first approach considered the usage of RSA algorithm with a 1024 bits key size on both mobile nodes and the WS itself. After public key exchange between the WS and a mobile node, all the exchanged information would be encrypted on the sender's side with the receiver's public key and decrypted with the receiver's private key. Although this option is completely valid to specific scenarios, it is necessary taking into account that RSA algorithm can only encrypt a limited amount of data that is directly related to the public key size. For instance, a 1024 public key can only encrypt 117 bytes, i.e., (1024/8) - 11 bytes.

eC4MHA aims any m-Health system, including applications that deal with different amounts of data. Therefore, this approach was not feasible and was discarded.

The second approach considered and applied in eC4MHA, is based on using a hybrid scheme to perform data confidentiality. The AES symmetric algorithm was chosen to encrypt all the data and the RSA asymmetric algorithm was used to exchange a random secret key used by the AES. It is assumed that an user is able to access directly (through Internet connectivity) the m-Health application WS. The reason for such assumption is the required exchange of the secret key between the WS and the mobile node before encryption can be performed, as may be seen in Figure 1. Therefore, the user is now able to securely retrieve health data, whether cooperation is required or not. Thus, the applied strategy assumes a secure transaction of data between nodes and the WS using the AES encryption algorithm in Cipher Feedback Mode (CFB), with a key size of 128 bits, and RSA algorithm with a 1024 bits keys size to exchange secret keys between nodes, and the WS.

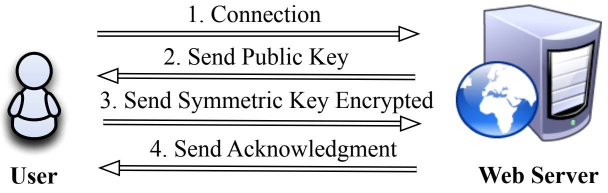


Figure 1 – Illustration of the Key exchange sequence on eC4MHA.

Integrity and authenticity

To assure authenticity, eC4MHA uses Message Digest 5 (MD5) algorithm in order to produce a 128 bits output, called message digest. To guarantee integrity, it uses the RSA algorithm to encrypt the message digest, commonly known as digital signature. The digital signature is then appended to the message that should be sent over the network.

Under this approach, cooperative mobile nodes should know their personal information that is being carried by messages sent all over the network, namely, the *requester control message* that contains user access credentials, such as username or password. A cooperative mobile node will merely act as a packet forwarder, until it reaches a mobile node with Internet connectivity. The mobile node is not aware of the packet content, other than required cooperative data such as node identification in order to forward back the response or reputation lists (RLs) determining and updating the level of cooperativeness of each mobile node. Through this proposal, it is assured that none of the sensitive information, such as login tokens or user's health information, is disclosed to unauthorized persons. Furthermore, it guarantees that information received is the original one as well as it comes from an expected and reliable source.

Key Management

Cryptography algorithms require encryption/decryption keys to operate. Therefore, it is vital to assure key's protection and privacy. This fundamentally depends on two factors, namely, where the keys are stored and who has access to them [16]. eC4MHA uses a *keystore* to store and assure key's protection and privacy. As above-mentioned, it is necessary to establish a previous connection to the WS in order to exchange a secret key for later communications. After a secret key generation, a *keystore* is created and the key is then securely stored and protected with a user password in the mobile device. To retrieve the secret key, the user must provide a password (in a transparent manner). Although the secret key is physically present in the device, it is not possible to access it from another application other than the application used to store the key. As for the WS, a *keystore* is also generated and used to store its own private key and each secret key needed for each node that requests data.

Figure 2 presents the overall and usual workflow of the eC4MHA in a cooperative environment. As may be seen, a requester node will try to discover and establish a connection to a mobile node through the above-mentioned cooperation mechanisms, receiving then a *node control message*. Then, a *requester control message* is sent to the requested node in order to define what information is it requiring. All the sensitive data is encrypted and signed. The requested node will then forward the request to the WS. The WS will receive the data, encrypting and signing it. The response is sent back to the request node forwarding it to the requester node that, after decryption, message integrity, and authentication verification will obtain the requested data.

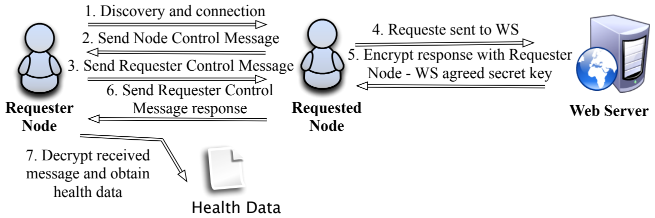

1. Discovery and connection
2. Send Node Control Message
3. Send Requester Control Message
6. Send Requester Control Message response
Requester Node
Requested Node
4. Requeste sent to WS
5. Encrypt response with Requester Node - WS agreed secret key
Web Server
7. Decrypt received message and obtain health data
Health Data

Figure 2 – Illustration of the eC4MHA overall workflow.

Performance Evaluation

This section focuses on the performance evaluation and validation of the m-Health cryptography proposal. An m-Health application, called SapoFit, was used to evaluate the performance of the proposed cryptography approach. The network scenario and expected node behaviors are also presented. Then, the validation and feasibility of the proposal is evaluated through a comparison with an early-proposed cryptography strategy, called DE4MHA, above described in Section II.

a. SapoFit Application

SapoFit is a weight control mobile application that allows users to keep track of weight [8-10]. It allows users to control their weight, body mass index (BMI), basal metabolic rate (BMR), sports activity, and the possibility to follow food plans based on their needed calories. In this m-Health application all the users must be registered in a Web service. For performance evaluation of eC4MHA, it is considered a user without Internet connection requesting access to the *Login* and *Food Plans* services. Therefore, the user *Profile* will be fully obtained through cooperation among nodes.

b. M-Health network scenario

An illustration of the real network scenario used for the performance evaluation study of the eC4MHA may be seen in Figure 3. It includes seven mobile nodes (using SapoFit), where three of them are assumed to be uncooperative nodes. Node M is the only node with available connection to the SapoFit Web services. Although this scenario may present mobility issues, for evaluation purposes, it is considered that each mobile node assumes the position presented in the network scenario.

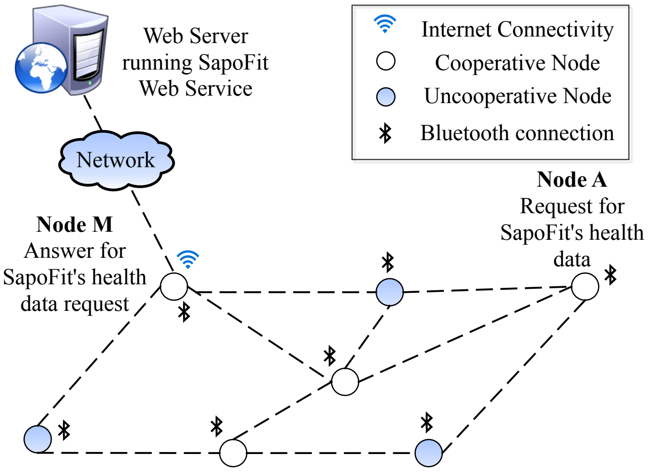

Web Server running SapoFit Web Service
Network
Internet Connectivity
Cooperative Node
Uncooperative Node
Bluetooth connection
Node M
Answer for SapoFit's health data request
Node A
Request for SapoFit's health data

Figure 3 - Illustration of the network scenario for performance evaluation of the eC4MHA.

The activity diagram of a mobile node is presented in Figure 4 It is subdivided into two logical parts: 1) Node discovery and connection and 2) *Cooperative Web Service*. The main goal consists in establishing a connection with the WS to obtain the required data. First, a node with no Internet connectivity and, therefore, unable to retrieve required data by itself, starts searching for neighbor nodes. If a node is found, cooperation information is exchanged among them, determining the cooperation status of the requested node as well what information it wants to retrieve. If the requested node is willing to cooperate, a *requester control message* is sent to the requested node. Sensitive information, e.g., passwords or health data, is encrypted with a secret key, shared uniquely between the requester node and the WS, and then signed with requester node's private key. This way, the cooperative node will not be able to access unauthorized information, but only strictly required information necessary to forward the request to the WS. As soon as the request arrives at the WS, it verifies the authenticity and integrity of the request. If both are verified, the required data is obtained by the WS and then encrypted with the previous referred key. Furthermore, the content of the message is also signed by the server in order for the requester node to check its integrity and authenticity. Later the message is sent to the requested node, with only the required information to decrypt.

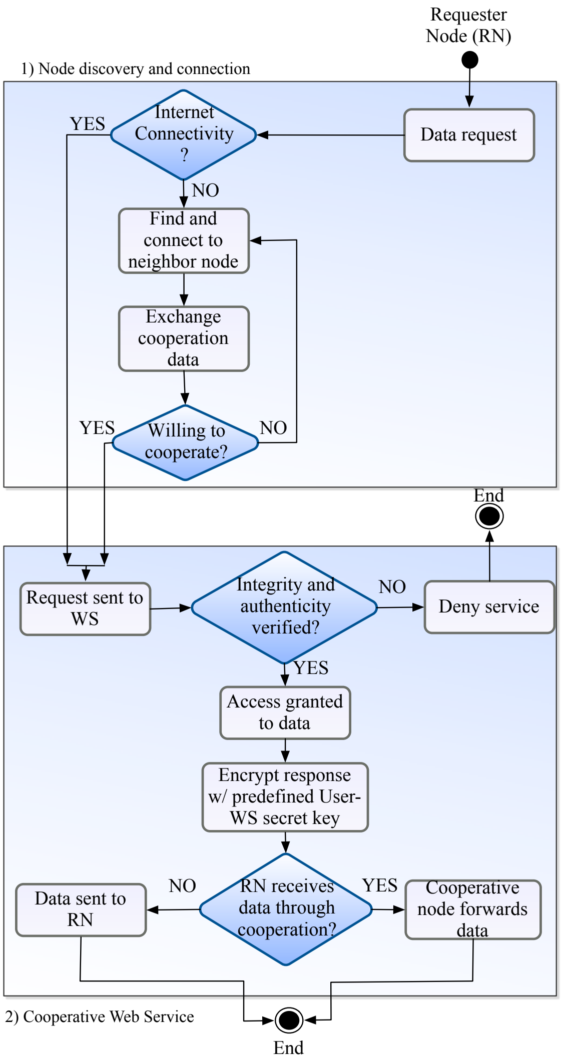

Requester
Node (RN)
1) Node discovery and connection
Data request
Internet Connectivity ?
YES
NO
Find and connect to neighbor node
Exchange cooperation data
Willing to cooperate?
YES
NO
End
Request sent to WS
Integrity and authenticity verified?
NO
Deny service
YES
Access granted to data
Encrypt response w/ predefined User-WS secret key
RN receives data through cooperation?
NO
YES
Data sent to RN
Cooperative node forwards data
2) Cooperative Web Service
End

Figure 4 - Activity diagram of a mobile node representing a mobile device with SapoFit and a typical node behavior.

c. *Performance Analysis*

This section focuses on the performance analysis eC4MHA through a comparison with an early-proposed cryptography strategy, called DE4MHA, above described in Section II.

The study was performed through a real m-Health application, called SapoFit. The case study scenario included seven devices running the SapoFit application. Non-cooperative cases were controlled and measured to worst case-scenario of three uncooperative nodes, to guarantee the minimum service performance. However, uncooperative nodes affect directly the service delivery probability, the service average delay, and the overall network performance. Hence, the first analysis refers to the performance comparison of the m-Health application with and without the used cryptography mechanisms. To obtain a comparison of both cases, performance metrics were considered, namely the service delivery probability and the service average delay (in seconds). The service delay is measured as the time between the request and its corresponding response. The service delivery probability and the service average delay in function of the number of uncooperative mobile nodes in both scenarios (with and without cryptography algorithms) are presented in Figures 5 and 6. As may be seen, cryptography algorithms degrade slightly the overall performance, as expected, due to more time consuming tasks, such as encryption and decryption. Furthermore, the service delivery probability presents similar results with cryptography algorithms. The variance reflects the use of eC4MHA in cases where whether integrity or authenticity is not guaranteed, resulting in a denial of service to the initial request, therefore, contributing to the decrease of the service delivery probability.

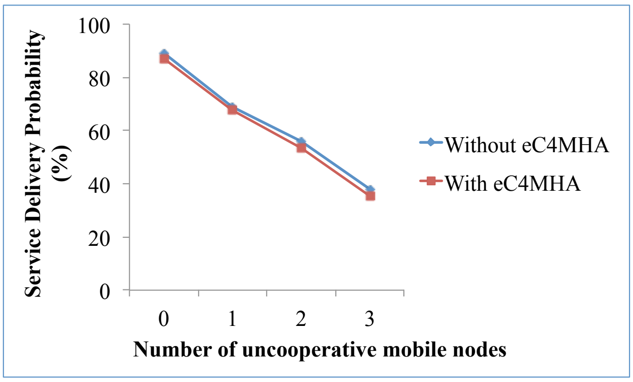


Figure 5 - Service delivery probability as function of the number of uncooperative nodes with and without eC4MHA.

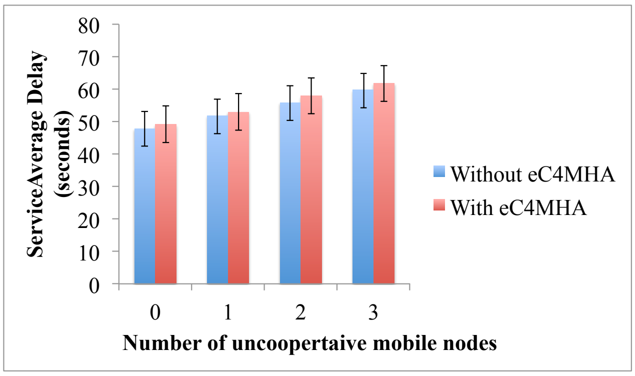


Figure 6 - Service average delay as function of the number of uncooperative nodes with and without eC4MHA.

The maximum service delay observed with three uncooperative nodes was about 59.8 seconds without eC4MHA with a standard deviation of 5.14 seconds, and about 61.8 seconds with eC4MHA, presenting a standard deviation of 5.57 seconds. These main variances were mostly caused by mobile devices constraints, such as loss of Bluetooth connection or distance variations among mobile nodes.

A performance evaluation analysis with the comparison to of both cryptography approaches for m-Health application, DE4MHA and eC4MHA was also considered and studied (Figure 7). Measuring the service average delay with both approaches it was demonstrated that eC4MHA is more effective and have better overall performance over DE4MHA.

Significant changes were made to the previous proposed strategy considering that each cooperative node would be aware of message content by turning them acting uniquely as packet forwarders in this new approach. Results show a slight improvement in the performance of service average delay with the eC4MHA. In a worst case-scenario with three uncooperative nodes, the requester node would receive the response to the request in about 64.06 seconds with DE4MHA and a standard deviation of 5.57 seconds while with eC4MHA an average of 61.8 seconds would be necessary in order to receive the response, with a standard deviation of 5.56 seconds.

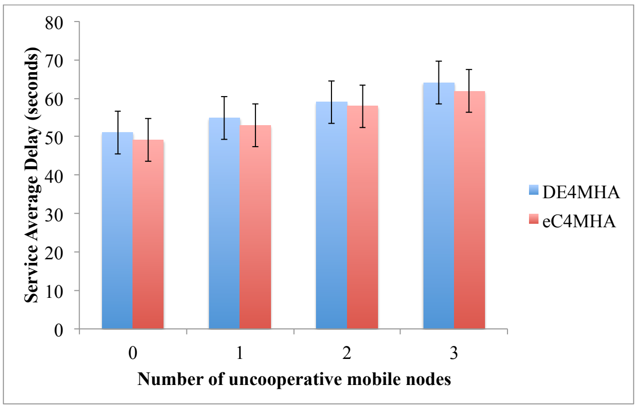


Figure 7 – Performance comparison of the service average delay in function of the number of uncooperative mobile nodes for DE4MHA and eC4MHA.

Conclusion and Future Work

This paper proposed a robust cryptography strategy for m-Health applications in a cooperative environment following a service-oriented architecture. This approach presented a solution where user health data is retrieved from a Web service through cooperation. It considers three main aspects: data confidentiality, data integrity, and data authenticity. The main objective of providing a cryptography solution for user's health data for m-Health applications in cooperative scenarios was fully accomplished. Another accomplished goal was the improvement of an earlier-proposed cryptography strategy, called DE4MHA, resulting in the eC4MHA.

The proposed solution was evaluated, demonstrated and validated through a real m-Health application, called SapoFit. Performance metrics were considered, such as service average delay and service delivery probability. The performance of the proposed eC4MHA was compared with DE4MHA. It was shown that it slightly increases service average delay and decreases service delivery probability. However, these results are totally feasible and tolerable in a real scenario and insignificant considering the assuring of privacy and security of the m-health data.

A comparison of both cryptography approaches and the respective performance evaluation through simulation, with different network scenarios and scalability, is also considered.

Acknowledgments

This work has been partially supported by *Instituto de Telecomunicações*, Next Generation Networks and Applications Group (NetGNA), Portugal, by National Funding from the FCT - *Fundação para a Ciência e a Tecnologia* through the PEst-OE/EEI/LA0008/2011 Project, and by the AAL4ALL (Ambient Assisted Living for All), project co-funded by COMPETE under FEDER via QREN Programme.

References

[1] S. Tachakra, X. Wang, R. Istepanian and Y. Song, " Mobile e-Health: the Unwired Evolution of Telemedicine," Telemedicine Journal and e-Health, vol. 9, nº 3, 2003, pp. 247–257.

[2] S. Akter, and P. Ray, "mHealth - an Ultimate Platform to Serve the Unserved," IMIA Yearbook of Medical Informatics, 2010, pp. 94-100.

[3] I. Cubic, I. Markota, and I. Benc, "Application of session initiation protocol in mobile health systems," presented at the MIPRO, 2010 Proceedings of the 33rd International Convention, Opatija, Croatia, May 24-28, 2010, pp. 367–371.

[4] G. Kramer, I. Maric, and R. D. Yates, "Cooperative communications (Foundations and Trends in Networking)," Now Publishers Inc., June 2007, ISBN-10: 1601980264.

[5] L. Buttyan and J.-P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad hoc Networks," Mobile Networks and Applications, vol. 8, nº 5, 2003, pp. 579–592.

[6] B.M.C. Silva, J.J.P.C. Rodrigues, I.M.C. Lopes, T.M.F. Machado, L. Zhou, "A Novel Cooperation Strategy for Mobile Health Applications," IEEE Journal on Selected Areas in Communications Special Issue on Emerging Technologies in Communications - eHealth, IEEE Communications Society (in press).

[7] B.M.C. Silva, J.J.P.C. Rodrigues, F. Canelo, I.C. Lopes, and L. Zhou, "A Data Encryption Solution for Mobile Health Applications in Cooperation Environments: DE4MHA", Journal of Medical Internet Research (JMIR), vol. 15, nº 3, 2013, DOI: 10.2196/jmir.2498.

[8] B.M.C. Silva, I.M. Lopes, P. Ray, and J.J.P.C. Rodrigues, "SapoFitness: A Mobile Health Application for continuous Monitoring Dietary Evaluation", 13th International Conference on E-Health Networking, Applications and Services (IEEE HEALTHCOM 2011), Columbia, MO, USA, June 13-15, 2011.

[9] J.J.P.C. Rodrigues, I.M.C. Lopes, B.M.C. Silva, and I. Torre, "A New Mobile Ubiquitous Computing Application to Control Obesity: SapoFit", in Informatics for Health and Social Care, Informa Healthcare, 2013 (in press).

[10] SapoFit, https://itunes.apple.com/pt/app/sapo-fit/id438487775?mt=8, Accessed in March 2013.

[11] T. Pering, Y. Agarwal, R. Gupta and R. Want, "CoolSpots: reducing the power consumption of wireless mobile devices with multiple radio interfaces," in MobiSys '06: Proceedings of the 4th international conference on Mobile systems, applications and services, Uppsala, Sweden, June 19 - 22, 2006, pp. 220-232.

[12] K. Raychaudhuri and P. Ray, "Privacy Challenges in the Use of eHealth Systems for Public Health Management," International Journal of e-Health and Medical Communications, IGI-Global, vol. 1, no. 2, pp. 12–23, 2010.

[13] R. Sulaiman, D. Sharma, W. Ma, and D. Tran, "A Security Architecture for e-Health Services," 10th International Conference on Advanced Communication Technology, Korea, February 17-20, 2008, pp. 99-104.

[14] M. Shanmugam, S. Thiruvengadam, A. Khurat, and I. Maglogiannis, " Enabling Secure Mobile Access for Electronic Health Care Applications," Pervasive Health Conference and Workshops, Innsbruck, Austria, November 29-December 1, 2006, pp.1-8.

[15] D. Brechlerova, M. Candik, "New trends in security of electronic health documentation," 42nd Annual IEEE International Carnahan Conference on Security Technology, Prague, Czech Republic, October 13-16, 2008 pp.13-16.

[16] M. Krishna, M. Doja, "Symmetric key management and distribution techniques in wireless ad hoc networks," International Conference on Computational Intelligence and Communication Networks (CICN), Gwalior, India, October 7-9, 2011, pp.727-731.