Ecosystem Analysis in the Design of Open Platform-based In-Home Healthcare Terminals towards the Internet-of-Things

Zhibo Pang[ab], Qiang Chen[b], Junzhe Tian[b], Lirong Zheng[b], Elena Dubrova[b]
[a]Corporate Research, ABB AB, Västerås, Sweden
[b]ICT School, Royal Institute of Technology (KTH), Stockholm, Sweden
pang.zhibo@se.abb.com

***Abstract*-In-home healthcare services based on the Internet-of-Things (IoT) have big potential in business. To exploit this opportunity, an ecosystem should be established first. Technical solutions should aim for a cooperative ecosystem by addressing the interoperability, security, and system integration. In this paper, we propose an ecosystem-driven design strategy and apply it in the design of an open-platform based solution. In particular, a cooperative ecosystem is formulated by merging the traditional healthcare and mobile internet ecosystems. Utilizing the existing standardization efforts, the interfaces between actors can be simplified. To balance the control and avoid monopoly, ecosystem-driven security schemes are proposed including the public-based authentication, repository-based credential management, SE-based cryptography, and non-invasive message handover. In order to achieve the economy of scale, an open platform-based in-home healthcare station is proposed. The proposed methodology and solution are demonstrated in implemented prototype system and field trials.**

Keywords- Ecosystem-Driven Design; Internet-of-Things; In-Home Healthcare; Open Platform; Android; Security;

I. INTRODUCTION

The revolution of Internet-of-Things (IoT) is reshaping the modern healthcare with promising economic and social prospects [1-3]. Powered by its ubiquitous identification, sensing, and communication capacities, all objects in the healthcare systems (people, equipment, medicine, etc.) can be tracked and/or monitored on a 24/7 basis [4]. Enabled by its global connectivity, all the healthcare related information (logistics, diagnosis, therapy, recovery, medication, management, finance, and even daily activity) can be collected, managed, and shared efficiently. By using the personal computing devices (laptop, mobile phone, tablet, etc.) and mobile internet access (WiFi, 3G, LTE, etc.), the IoT-based healthcare services can be mobile and personalized [5-7]. Large user base and maturated ecosystem of traditional mobile internet service have significantly sped up the development of the IoT-powered in-home healthcare (IHH) services, so-called Health-IoT. At the same time, the Health-IoT extends the traditional mobile internet services to a new application area. Especially after the open-source operation systems, such as Android [8], were introduced and broadly applied, the Health-IoT has been expected to be one of the "killer" applications of IoT. Therefore the development of Health-IoT solution based on open platform has become a hot topic.

In recent years, a number of single point devices and applications have been proposed. But as required by the economy of scale, a general architecture is needed to support various applications by a common IoT platform. So, more comprehensive architecture study is needed. Moreover, this general architecture should be feasible not only from technical point-of-view but also from business point of view. Comparing to the traditional mobile internet ecosystem, the Health-IoT ecosystem is much more complicated as more stakeholders are involved. To create sustainable Health-IoT services, the establishment of a cooperative ecosystem is primarily important to the whole industry. Such ecosystem should deliver enough added values to all stakeholders instead of a part. High level architectures of all technical aspects such as security, interoperability, and enterprise information system (EIS) integration, should serve for this goal. Therefore, ecosystem-driven design strategy is necessary in the early stage of technical development. The exiting research on this topic is very rear.

In this paper, we propose and demonstrate an ecosystem-driven design strategy for the Health-IoT applications. In particular, a cooperative ecosystem of Health-IoT is formulated first based on the analysis of the traditional healthcare and mobile internet ecosystems. As it is established upon shared infrastructures, the interoperability of devices from different suppliers is important. By reviewing existing standardization efforts on device interoperability, we propose a set of simplified interfaces among different actors within the ecosystem.

Secondly, in order to achieve the economy of scale, an IHH Station (IHHS) is proposed as a universal platform for device and service integration and convergence. To protect the benefits of all stakeholders, value-centric security schemes are proposed, including the public authority-based authentication,

the secure element (SE) based cryptography, and the non-invasive message handover.

Thirdly, to verify the concepts and technical feasibilities, we have developed a prototype system called iMedBox. It is a specific case for medication management and in-home monitoring applications. The iMedBox hardware, software and backbone system are implemented and evaluated by field demonstrations. The positive feedbacks have proven the feasibility of proposed design methods, proposed architectures and solutions. Based on the results of this paper, economically feasible services are closer to reality.

The rest of this paper is organized as follows. The ecosystem analysis and technical interfaces are presented in section II. The security schemes are presented in section III. The IHHS architecture, implementation, and experimental results are introduced in section IV, and concluded in section V.

II. To Establish a Cooperative Ecosystem

A. *Lessons from Google Health's failure*

Since Jan 1, 2012, as one of the most famous Health-IoT business efforts, the Google Health service has been discontinued [9]. This has been looked as a big setback. It is difficult to assert the exact reason but we can learn some lessons by analyzing the possible reasons. According to the summary of possible reasons listed by Brian Dolan [10], seven of the ten reasons are related to the establishment of ecosystem: the Google Health was *not trustworthy* (lack of public authority), *not fun or social*, *not involving doctors*, *not partnering with insurance companies*, *hard to overcome the current reimbursement barriers*, *lack of advertising opportunity*, and *not useful to consumers*.

This finding is consistent with the prediction of ITU when the vision of IoT was introduced: "*the Internet of Things will occur within a new ecosystem that will be driven by a number of key players*" [11]. Before developing the technical solutions, it is more important clearly answer "*how to establish a new cooperative ecosystem, and how to deliver enough added values to all of stakeholders in that ecosystem?*" Hence, the ecosystem analysis is the first step of our work.

B. *Ecosystems of traditional healthcare and mobile internet*

As shown in Fig. 1 (a) and (b), the ecosystems of traditional healthcare service and traditional mobile internet service are formularized and compared. The main stakeholders involved in both of them can be classified into four roles: financial sources, means suppliers, service providers, and end users. The service providers are the actor of service execution and delivery. Means providers provide necessary materials, tools, supplies, etc. to the service providers but seldom face the end users directly. Products and services mainly flow from means providers, through service providers, to end users. Payments (obligatory or optional, depending on different cases) flow back from end users, through financial sources, to the means providers and service providers. Thus a close-loop value chain is established. It is exactly the "close-loop" feature that makes the ecosystem economically sustainable. Win-win cooperation is enabled only if every stakeholder's benefit is guaranteed.

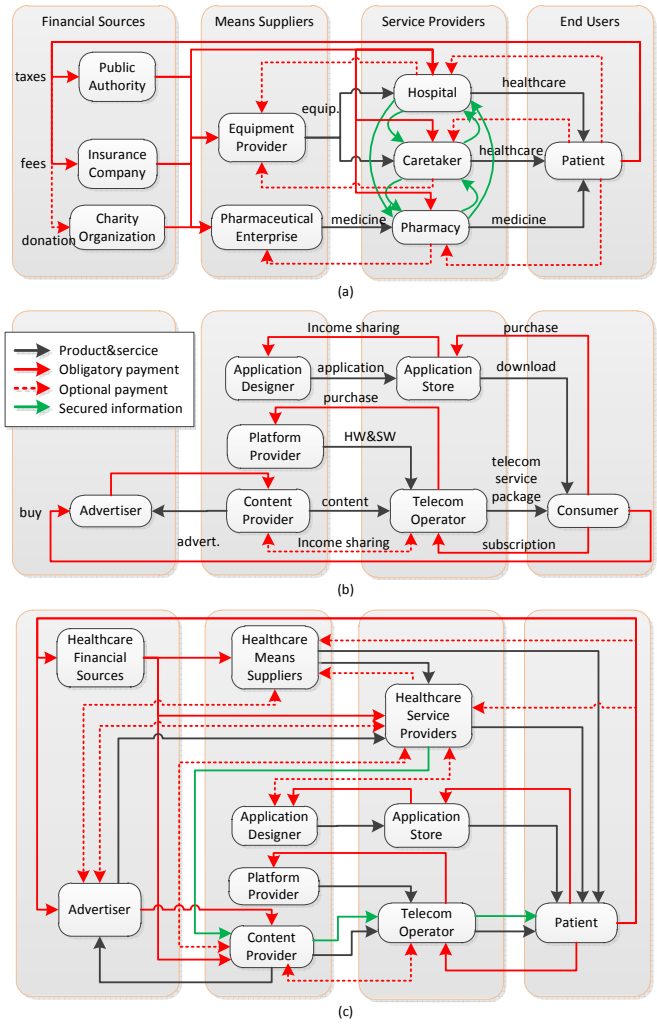

Fig.1. Business ecosystems of (a) traditional healthcare service, (b) traditional mobile internet service, and (c) IoT-powered healthcare service

In spite of the above mentioned similarity, we can see significant differences between the two ecosystems. Firstly, the healthcare service ecosystem has more complicated financial sources. Despite the diverse policies in different countries, the public authority and insurance company are the most important financial sources, and thus have the highest influence on the rules of healthcare services. Another important difference is related to privacy and security. The healthcare services deal with privacies of end users which are much more sensitive than that in the mobile internet services. As a result, in the traditional healthcare ecosystem, the privacy information flows within the service providers strictly limited by regulations that have been well established and accepted. These two major differences are the main concerns and drivers when we formulate the new Health-IoT ecosystem.

C. *The proposed ecosystem*

As shown in Fig. 1 (c), the new IoT-powered healthcare service ecosystem is proposed and formulated by merging the two traditional ecosystems. Obviously the Health-IoT service is a business upon shared infrastructures including the internet backend facilities, core networks, access networks, and mobile terminals.

In this ecosystem, the healthcare service providers (like hospitals, elderly houses, pharmaceutical enterprises etc.) and healthcare financial sources (like public authorities, insurance companies, etc.) have larger influence than other stakeholders. The content providers (like Google, Amazon, Facebook, etc.) and telecom operators (like China Mobile, Vodafone, Verizon, etc.) cannot rule the ecosystem anymore. Large mobile device providers (like Apple, Nokia, Samsung, etc.) and medical device providers (like Roche, Omron, Philips, Johnson, etc.) should cooperate more than before to ensure the interoperability of their products. Due to the application-store-based software distribution model, consumers and application developers get more fairness in the ecosystem.

The cooperation between traditional healthcare service providers and internet content providers is the key to bring the ecosystem into reality. On one hand, the healthcare service providers don't need to establish new extra infrastructures (like data centers, servers, software and other backend systems) by their own. Instead, they should make use of the existing infrastructures owned by the internet content providers. In this case, the contents of healthcare services are delivered to the end users through the channels of telecom operators. On the other hand, the internet content providers, as well as telecom operators, should get the healthcare contents from healthcare service providers rather than "create" such contents by themselves. The healthcare financial sources should encourage and protect such cooperation by paying to the content providers directly or through healthcare service providers.

Furthermore, the privacy regulations and public authentications should be applied to the content providers and telecom operators, as strictly as they are applied to the healthcare service providers. This is the primary precondition for the end users to agree on uploading and managing their privacy through these channels. Besides the legislative approaches, technical approaches should also be in place to make sure only the owner and specially authorized individuals can access the private information. These principles are the foundation of the proposed security schemes.

Additionally, the advertisers should be authorized to provide specific advertisement services for both healthcare means providers and healthcare service providers. But this advertisement shouldn't invade any patient's privacy. It is important to be aware that advertisement is the most mature and trusted business model of the mobile internet ecosystem. Respect on such well-established business model is essential to initiate new businesses.

D. *Standardization of the interfaces*

Given the formulation of the new Health-IoT ecosystem, specific technical requirements can be derived more comprehensively and clearly. For example, the standardization of interfaces between any two actors within the ecosystem are necessary to ensure interoperability. The standardization of Health-IoT technologies should be ecosystem-driven instead of technology-driven.

As shown in Fig. 2, three types of interfaces should be standardized. Firstly, the hardware and software interfaces between healthcare means suppliers and mobile application designers, and between means suppliers and mobile platform providers. For these interfaces, the Continua Health Alliance (CHA), a major standardization body working on device level interoperability, has recommended the Bluetooth Health Device Profiles (HDP), USB Personal Healthcare Device Profile and ZigBee Health Care Profile. They all apply a common data format specified by the ISO/IEEE 11073 family. Based on these standards, the mobile platform providers and application designers can make a common driver for the same class of medical devices from different manufacturers. And then, the mobile devices can recognize a particular medical device according to its hardware descriptor and automatically apply correct data parsing and communication protocols. Thus, the complexity of patients' operation, hardware and software costs, and hence time to market, can be significantly reduced.

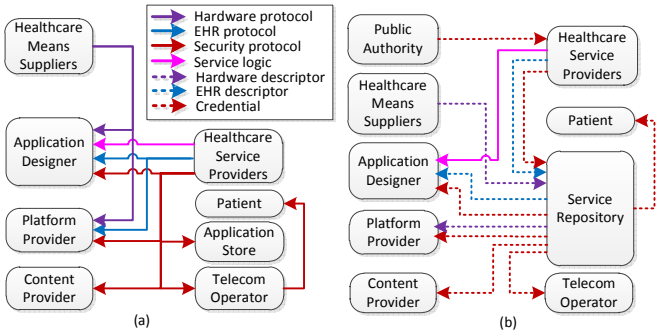

Fig.2. Technical interfaces between actors (a) without standardization, and (b) with standardized hardware interfaces, data formats, and security schemes

Secondly, the format of electronic health record (EHR) should be standardized. The HL7, EN 13606 (specified by European Committee for Standardization), and ISO 18308 are the major efforts for this purpose. These EHR standards define 1) the protocol to exchange EHR messages; 2) the contents and structures EHR data, and 3) the mechanisms to ensure privacy and security of information sharing. By applying the EHR standards, the technical negotiations between healthcare service providers and mobile platform providers are simplified or hopefully avoided. The negotiation between healthcare service providers and application designers are simplified too.

Thirdly, security schemes throughout the entire ecosystem should be standardized. Otherwise, all the parties would certainly intend to specify their own security mechanisms to

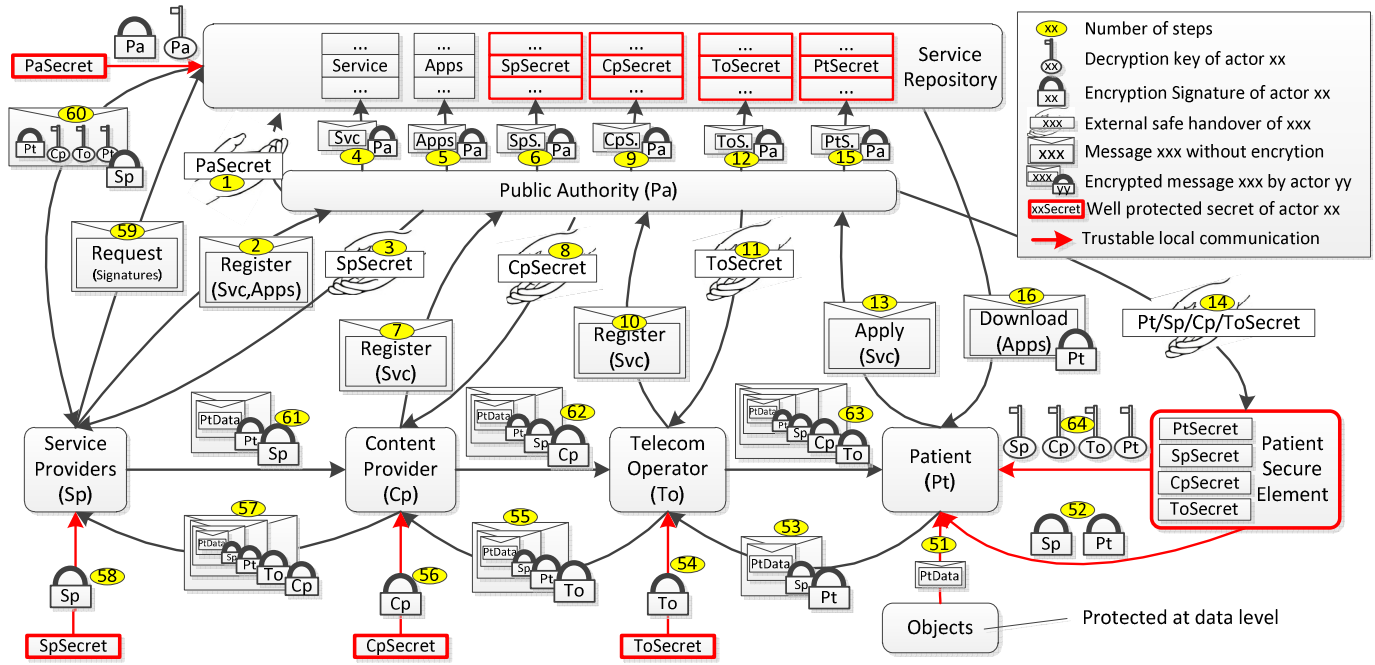

Fig.3. The proposed security schemes

protect their information as well as business benefits. However, the existing standardization efforts have not provided a solution so far. In our solution, to be trusted by the whole ecosystem, the traditional application store should be accredited by public authorities, and then it is transformed into a service repository. All security credentials are recorded by the repository and supervised by the public authority.

It is necessary to mention that the service logic should be left proprietary instead of standardized to encourage differential competition. The healthcare service providers can customize proprietary apps from application designers to accomplish specific value-added services. This point is supplementary to the efforts of IHE which promotes the coordinated use of established standards such as HL7 to address specific clinical need in support of optimal patient care.

III. Ecosystem-driven Security Mechanism Design

A healthy ecosystem should protect the benefits of all stakeholders by balancing the control and avoiding monopoly. In the Health-IoT ecosystem, security mechanisms are the primary technical means to do so (of course, there are many non-technical measures that should be applied, but they are out of the scope of this paper). As the patients never believe the content providers and telecom operators can really protect their privacy [10], the only solution is to accredit an independent mediator, here the service repository, by the public authority. Principally, only the owner of the private information (the patient and his/her healthcare service provider) can access the information.

Based on the above considerations, the security schemes are proposed in Fig. 3. The public authority, service repository, healthcare service provider, content provider, telecom operator, and patient are the main actors in these security schemes.

A. *Public-based authentication*

As illustrated by the step1~14 in Fig. 3, to launch a particular Health-IoT service to the market, the enterprises should get authentication from the public authority first. The authentication is granted in the form of credential, so-called Secrete, which is a set of cryptography software running in the trusted hardware. The Secrete of each actor should be handed over by superior and safe approach. For example, it can be registered and delivered in person and delivered by accredited couriers. Only a certain person of a certain service provider can access a certain patient's information. That is, the authentication is tied to individuals instead of organizations.

B. *Repository-based credential management*

The service repository maintains all the Secretes of actors in trusted facilities. The content provider and telecom operator only maintain their own Secrets, which ensures the non-invasive message handover in-between patient and healthcare provider. The service provider maintains its own Secrete locally and can request other actors' keys from service repository.

C. *SE-based cryptography*

The secure element (SE) is a secured device that can store and execute specific cryptography algorithm. The algorithm is written by issuer and is extremely difficult to hack. A typical SE is the SIM (subscriber identification module) card that is

commonly used in mobile telecom services [12]. When a message is sent from the sender, it is encrypted and a signature is attached. Both the encryption key and signature are generated dynamically by the sender's SE. When the receiver receives the message, it sends the signature to its own SE. If the receiver has been authorized, there should be a copy (symmetric or asymmetric) of the sender's Secret in the receiver's SE, so that the receiver's SE can derive the decryption key. Only if everything (the signature, encryption key, decryption key, and Secrets in the SEs of both-sides) matches, the message can be decrypted. Furthermore, the Secrets in the SE are readable and writable only by the issuer (here the public authority). So, although the patient's SE contains the Secrets of other actors, the Secrets are not disclosed. And the communication between apps and SE is local within professional equipment (e.g. the Health-IoT Station). This reduces the security risk further.

If the SIM card is used as the SE, the logistics of SIM-card management will be significantly different with that in traditional telecom services. Traditionally, the SIM card is fully issued and supervised by the telecom operator. But in Health-IoT services, the SIM card should be issued and supervised by the public authority, and the telecom operator can only manage a part of the SIM as predefined by the public authority. This change may cause resistance by telecom operators. It should be resolved mainly by non-technical means, such as policy enforcement and financial compensation. And the telecom industry has also prepared technical solutions such as the remote subscription and SIM supervision [13].

D. Non-invasive message handover

The information from patient to service provider and response from service provider to patient are illustrated in the step 51~60 and step 61~64 respectively. As the content provider and telecom operator only maintain their own Secrets, they have no access to the messages transmitted through their facilities. In other words, the Health-IoT streams are transparent to them. This mechanism is called non-invasive message handover which is essential to get trusted from the end users and financial sources.

IV. ECOSYSTEM-DRIVEN TERMINAL DESIGN

A. The IHH Station as the common terminal platform

As a typical shared infrastructure, the IHHS is not a close system. Instead, it should be open to other applications like telecommunication and entertainment, so that the content suppliers and telecom operators can deliver other value-added services through it. Solid security is ensured by the secure element which could be the SIM card, the NFC (near field communication) card, or an embedded secure device.

The proposed IHHS solution is based on open source operation systems like the Google Android. It uses standard mobile internet terminal hardware, such as tablet PC, provided by various 3C (consumer, communication and computing) manufactures. By installing specific apps, the 3C terminal can transform into many variants, from the logbook, to fatal monitor, wheel chain controller, portable monitor, smart walker, and medicine box (Fig.5). It is suitable for mass production with low cost as it is a "*standard"* product. It is also broadly acceptable by the whole ecosystem as it is based on an "*open*" platform.

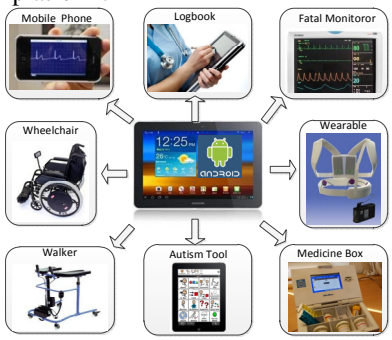

Fig.4. Hardware variants of the Health-IoT Station based on open platform

B. The Concept of the iMedBox

To verify the concepts and design strategy proposed in this paper, a prototype system has been implemented and evaluated in field trials. As a typical case of the IHHS, application scenario of an iMedBox system has been proposed in our previous work [14]. A powerful intelligent medicine box (iMedBox) works not only as in-home medicine container, but also as a "*medication inspector*", and an "*onsite examiner*" in daily healthcare monitoring. It connects to the healthcare service providers through 3G and WiFi networks and communicates to medical devices through USB, NFC, RFID, and WSN (wireless sensor network). Medication and fatal information is transmitted to the backbone systems and feedback from service providers is presented to the patient at home. The iMedBox is equipped with touch screen and powerful processors to provide friendly user interface and best operation fluency.

C. Implementation of the IHHS prototype

The prototype is based on the Samsung Galaxy Tab10.1 tablet PC. It has a 10.1 inch display with touch screen, a dual-core 1GHz ARM Cortex-A9 CPU, and connections through USB OTG, WiFi and 3G. The operation system is Android 3.1. As shown in Fig. 4, we extended the hardware through a USB adaptor to support NFC and WSN connections which are not standard peripherals of tablet PC so far. A functional iMedBox is assembled by embedding the tablet and extension modules into a hand-molding box. As a part of the demonstration, intelligent medicine packages are made by attaching inlay RFID tags onto ordinary medicine packages.

The application software for the demonstration is implemented in Java as standard Android apps. The graphic engine is the AChartEngine, and database engine is the SQLite. A dedicated data processing engine for data packet parsing, a security engine for authentication and cryptograph, and a web server for 3G/WiFi connection are implemented based on the

basic Android 2.1 API which is supported by major variants of Android. Two types of GUI are designed so far: a Sensor View for sensor data and a Medication View for prescription.

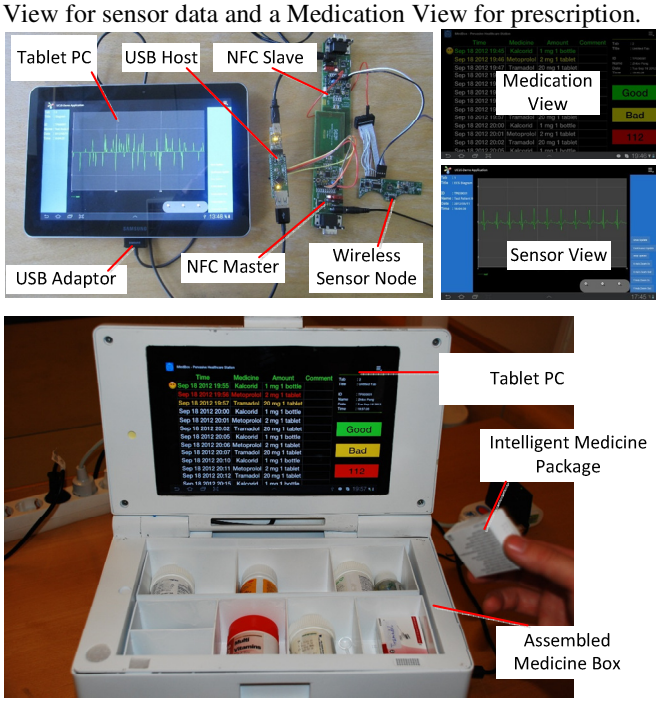

Fig. 5. Implementation of iMedBox prototype

D. Users' feedback and improvement directions

Some field trials have been carried out in nursing centers and elderly houses in Blekinge, Sweden. The system concepts have been confirmed by the positive feedback. The medication reminding and recording functions can significantly improve the medication compliance especially for elderly. Seamless integration to the hospital's prescription system is necessary to reduce the workload of manual input. The proposed authentication scheme sounds complicated but necessary to reassure the users.

Some insufficiencies are also pointed out. The user interfaces are still too complicated for elderlies although they are acceptable for nurses. The texts are not clear enough. This can be improved by replacing the Android's default colors and fonts which is quite "fashion" but lack of clarity. The network connection and authentication are too slow (currently around 10 seconds). We will further measure the latency step-by-step to find out the bottleneck and improve.

V. CONCLUSION AND FUTURE WORK

To develop successful Health-IoT solutions towards the IoT, a cooperative ecosystem should be established first. Technical architectures should be centered to the ecosystem especially regarding the interoperability, security and information system integration. In this paper, a cooperative ecosystem of Health-IoT is formulated based on the analysis of the traditional healthcare and mobile internet ecosystems. Then we apply the ecosystem-driven strategy in the design of security mechanisms and terminal platform. To balance control ability and avoid monopoly, ecosystem-driven security schemes are proposed including the public-based authentication, repository-based credential management SE-based cryptography, and non-invasive message handover. In order to achieve the economy of scale, an Android-based in-home healthcare station is proposed to be the convergence terminal platform. To verify the concepts, we implemented an iMedBox prototype as a specific application case. The positive feedback from field trials has proven the effectiveness of proposed methodology and solutions. Improvement directions are also pointed out such as speed of authentication, fluency of operations, and clarity of graphical user interfaces.

One important future work is to implement the proposed security mechanisms by involving more external partners including the SIM card maker and telecom operator. Then we plan to integrate the iMedBox terminal into some existing healthcare information systems and carry out more trials.

REFERENCES

[1] Daniele Miorandi, et al. "Internet of things: Vision, applications and research challenges", *Ad Hoc Networks*, online 21 April 2012

[2] Mari Carmen Domingo, "An overview of the Internet of Things for people with disabilities", *J. Network and Computer Applications*, 35(2), March 2012, 584-596

[3] Dohr, A.; et al. "The Internet of Things for Ambient Assisted Living", *Int. conf. information Technology: New Generations*, 2010, 804 – 809

[4] Hande Alemdar, Cem Ersoy, "Wireless sensor networks for healthcare: A survey Original", *Computer Networks*, 54(15), 2010, 2688-2710

[5] Chang Liu, et al. "Status and trends of mobile-health applications for iOS devices: A developer's perspective" *J. Systems and Software*, 84(11), November 2011, 2022-2033

[6] Predrag Klasnja, Wanda Pratt, "Healthcare in the pocket: Mapping the space of mobile-phone health interventions", *J. Biomedical Informatics,* 45(1), 2012, 184-198

[7] Inmaculada Plaza, et al. "Mobile applications in an aging society: Status and trends", *J. Systems and Software,* 84(11), 2011,1977-1988

[8] Google Android operation system, http://www.android.com

[9] Google Health, www.google.com/health, accessed on May 12, 2012.

[10] Brian Dolan, "10 Reasons why Google Health failed", *MobiHealthnews by Chester Street Publishing, Inc,* Jun 27, 2011

[11] ITU, "The Internet of Things-Executive Summary", www.itu.int, 2005

[12] Kalman, G.; Noll, J.,"SIM as Secure Key Storage in Communication Networks", *Int. conf. ICWMC*, 2007, 55 – 55

[13] Luis Barriga, et al. "M2M Remote-Subscription Management", *Ericsson Review* 2011 (1)

[14] Zhibo Pang, Qiang Chen, Lirong Zheng, "A Pervasive and Preventive Healthcare Solution for Medication Noncompliance and Daily Monitoring", *2nd Inte. Symp. on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2009)*, pp1-6, Nov. 2009,