Ecosystem-Driven Design of In-Home Terminals Based on Open Platform for the Internet-of-Things

Zhibo Pang*, Junzhe Tian**, Qiang Chen**

*Corporate Research, ABB AB, Västerås, Sweden

** ICT School, Royal Institute of Technology (KTH), Stockholm, Sweden

pang.zhibo@se.abb.com, {junzhe, qiangch}@kth.se

***Abstract*—In-home healthcare services based on the Internet-of-Things (IoT) have great business potentials. To turn it into reality, a business ecosystem should be established first. Technical solutions should therefore aim for a cooperative ecosystem by meeting the interoperability, security, and system integration requirements. In this paper, we propose an ecosystem-driven design strategy and apply it in the design of an open-platform-based in-home healthcare terminal. A cooperative business ecosystem is formulated by merging the traditional healthcare and mobile internet ecosystems. To support the ecosystem in practical technology and business development, ecosystem-driven standardization efforts, security mechanisms, terminal design principles, and data handling schemes are analyzed and corresponding solutions or guidelines are presented. Thirdly, to verify the proposed design strategy and guidelines, an open-platform-based terminal is implemented and demonstrated by a prototyping system.**

***Index Terms*—Ecosystem-Driven Design; Internet-of-Things (IoT); In-Home Healthcare Station (IHHS); Open Platform;**

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 the 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 developed. But as required by the economy of scale, a generic architecture is needed to support various applications by a common IoT platform. So, more comprehensive 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 rare.

In this paper, extending our previous works in [14-18], an ecosystem-driven design strategy for the Health-IoT applications is presented and demonstrated.

First, a cooperative ecosystem of Health-IoT is formulated by Value Chain Analysis of the traditional healthcare and mobile internet ecosystems. The two traditional business ecosystems are destructed and merged into one new ecosystem.

Second, as the ecosystem of Health-IoT is established upon

Manuscript received July 29, 2013. This work was supported in part by the VINN Excellence Center of iPack at the Royal Institute of Technology.

Zhibo Pang is with ABB AB, Corporate Research, Forskargränd 7, 72178, Västerås, Västmanland, Sweden (phone: +46-21 325104; fax: +46-21 323212; e-mail: pang.zhibo@se.abb.com).

Junzhe Tian and Qiang Chen are with Royal Institute of Technology, Department of Electronic Systems, Isafjordsgatan 39, 16440, Kista, Sweden. (e-mail: {junzhe, qiangch}@kth.se).

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.

Third, to support fair distribution of benefits among 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.

Forth, 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. Design principles of the open-platform-based terminals are detailed.

Fifth, ecosystem-driven data handling schemes are introduced including layered data compression and self-contained data formatting.

Finally, 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 is presented in section II. The standardization efforts are reviewed in section III. The security schemes are presented in section IV. The design principles of open-platform-based terminals are given in section V. The data handling mechanisms are introduced in section VI. The implementation of the prototyping system and experimental results are discussed in section VII, and concluded in section VIII.

II. Ecosystem Reconstruction

A. Lessons from the failure of Google Health

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.

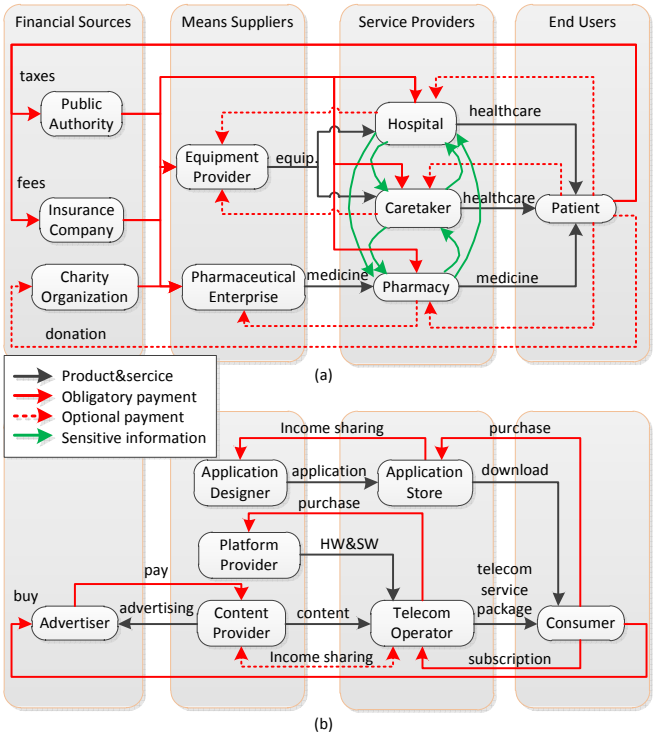


Fig.1. Business ecosystems of (a) traditional healthcare service, (b) traditional mobile internet service

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 Health-IoT ecosystem*

As shown in Fig. 2 the new Health-IoT ecosystem is proposed and formulated by merging the two traditional ecosystems. Obviously the Health-IoT service is a business established on shared infrastructures including the internet backend facilities, core networks, access networks, and mobile terminals.

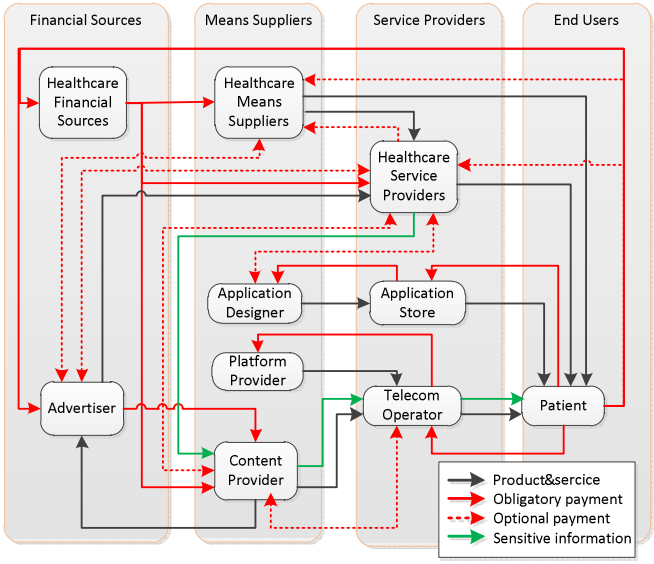


Fig.2 The proposed cooperative ecosystem of the Health-IoT service

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.

III. Ecosystem-Driven Standardization Efforts

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. 3 three types of interfaces should be standardized.

A. *Interoperability of devices*

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.

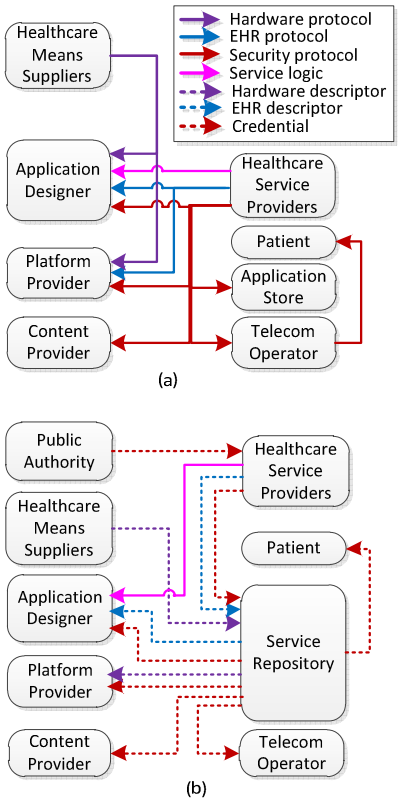


Fig.3 Technical interfaces between actors (a) without standardization, and (b) with standardized hardware interfaces, data formats, and security schemes

B. *Electronic health record (EHR)*

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.

C. *Uniform security mechanisms*

Thirdly, security schemes throughout the entire ecosystem should be standardized. Otherwise, all the parties would certainly intend to specify their own security mechanisms to protect their information as well as business benefits. However, the existing standardization efforts have not provided a solution so far. The root-cause is, the motivation of these standardization efforts on the security aspects is opposite to the "cooperative ecosystem". Device vendors and service providers mostly prefer to keep the security mechanisms to be proprietary aiming for the so-called "vendor lock-in". Unfortunately, it is the market itself that is "locked"!

In the solution that will be presented in the next section of this paper, 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.

D. *Keep the service logic proprietary*

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.

IV. Ecosystem-Driven Security Mechanisms

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. 4 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 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

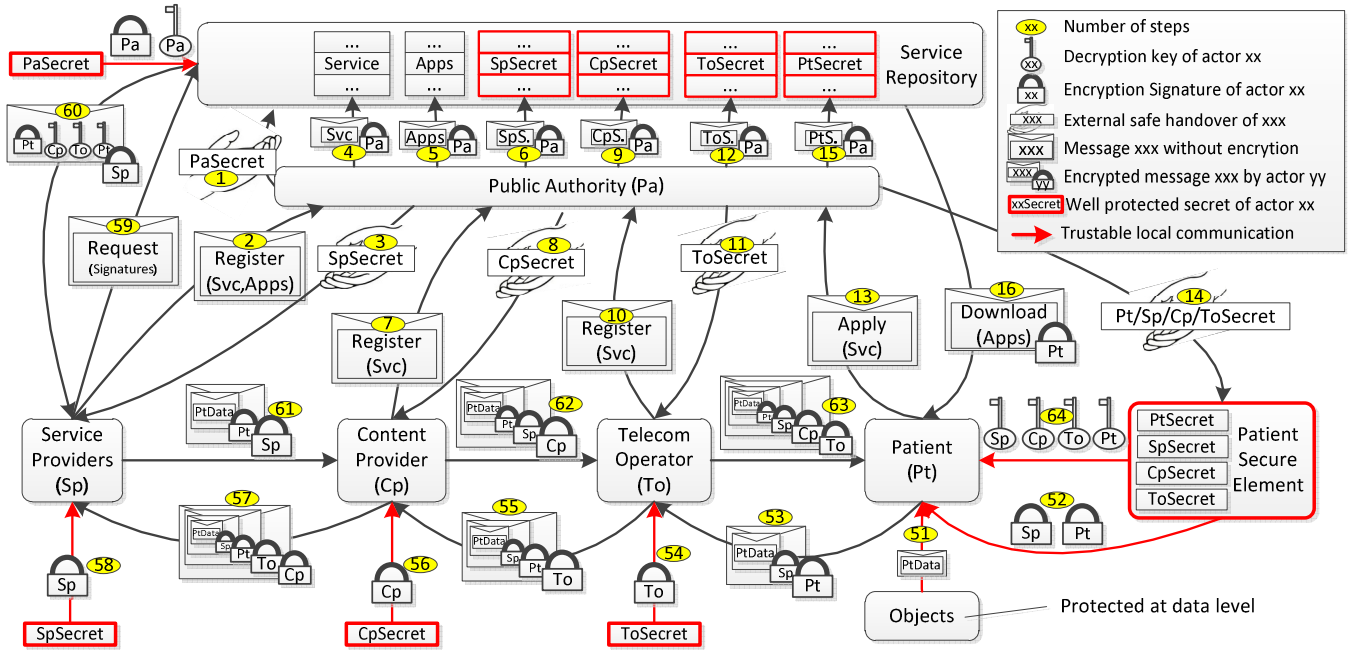


Fig.4 The proposed security schemes

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.

V. ECOSYSTEM-DRIVEN TERMINAL DESIGN

In order to establish the proposed Health-IoT ecosystem, the in-home healthcare station (IHHS) is the most important infrastructure that can be shared by all actors in the ecosystem. Therefore it should not be a close system. Instead, it should be open to third party applications like telecommunication and entertainment, so that e.g. the content suppliers and telecom operators can deliver other value-added services through it.

By installing specific apps, the IHHS 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.

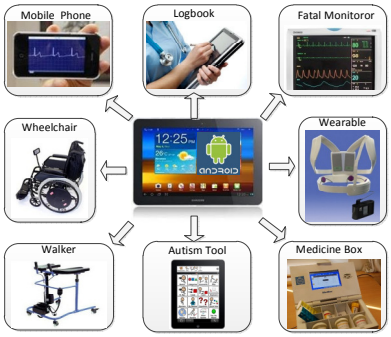


Fig.5. Hardware variants of the Health-IoT Station based on open platform

Before look into the technical details, several design principles for the terminal should be clarified first. These

principles are the foundation for the design of hardware and software architectures of a particular solution. More details are also presented in a previous article [15].

A. Common platform based on 3C products

As required by the business ecosystem, the terminal hardware should be based on a mass produced 3C (computing, communication, consumer) platform such as mobile phone and tablet PC. The huge volume of 3C products has significantly minimized the development costs. The latest semiconductor and software techniques are adopted timely. So the IHHS providers can introduce their products with the shortest time-to-market and best performance-to-cost ratio. Performance, user experience, and maturity of developer community are the criteria for the platform selection. Well established software distribution channels are also important to establish the proposed Health-IoT ecosystem.

B. Certification of the Health Extension

The IHHS provider needs to customize the specific parts, so-called the Health Extension, of the terminal. These parts are not standard peripherals in the 3C platform, e.g. some specific mechanical structures and interfaces to biomedical sensors and device. The Health Extension is the importance entrance for the healthcare service providers and public authorities to be involved in the Health-IoT ecosystem. So, the IHHS provider must cooperate with them to offer a complete solution. In particular, the healthcare service providers can customize proprietary Health Extension based on their know-how and service contents. Only the certified products can access their contents. The public authorities can specify regulations to certify the Health Extension. Only the certified products and services can get the financial supports, such as the reimbursement of cost. This is an important technical measure to guarantee the Health-IoT is under public supervision.

C. Interoperability and extendibility

Devices from third parties are integrated to the IHHS through the device adaptors in the Health Extension. The aforementioned standardized interfaces for devices from various vendors should be supported, such as the ones recommended by the Continua Health Alliance: the Bluetooth Health Device Profiles, USB Personal Healthcare Device Profile and ZigBee Health Care Profile. However the IHHS developers cannot expect one single interface can fit all devices. Most of the popular interfaces should be supported such as USB, Bluetooth, WiFi, NFC (near field communication), RFID, WSN, etc. At the same time, extendibility for future standards should be reserved too.

D. Convenient and trusted software distribution

The application software for a particular Health-IoT service should be distributed through the application stores which have essentially enabled the mobile internet ecosystems. It is friendly both to the users and to the apps developers. The drivers for the Health Extension should be either natively integrated in the 3C platform or installed together with the apps, so that the device and service can be plug-and-play. At the same time, the publishing and installation of Health-IoT should be supervised by the public authorities. So the IHHS solution should provide trusted user identification, authentication and payment mechanisms e.g. through secured NFC interface. Solid security is ensured by the secure element which could be the SIM card, the NFC card, or an embedded secure device.

E. Standardized and secured EHR handling

The handling of EHR data is the center of information and service integration. For this purpose, a virtual local database is necessary to isolate the apps from different parties. The format of data exchanged between devices, apps, and backend systems should follow international standards such as the ISO/IEEE 11073, EN 13606, and ISO 18308 specifications. At the same time the access of EHR data should be authorized and controlled strictly, e.g. complying with the mechanisms proposed above.

F. Efficient service composition

The service oriented architecture (SOA) has been broadly adopted in the integration of healthcare services [15]. But to execute the intensive SOA middleware on the mobile platform is still challenging. State-of-the-art simplification and optimization are necessary.

G. Efficient information integration

The IHHS needs to efficiently process not only the vital signals from biomedical sensors but also the human activities collected by many other sensors such as microphone, camera and infrared sensor. The processing of multimedia data and diagnostic analysis of vital signals are computation-intensive. The popularity of multicore processors in 3C platforms has made it possible to perform such intensive tasks on a low cost IHHS [14]. Correspondingly, the terminal software architecture should be optimized to make the best use of the parallel computation capacity of multicore processors. This will be further introduced in the next section.

VI. Ecosystem-Driven Data Handling

A. Data flows

As shown in Fig.6, the main data flows between the three parts of a Health-IoT system, the service backend, local station, and sensor devices are illustrated. The raw data are collected by the sensor devices with more or less compression because of the low processing performance of the sensor nodes. Here needs a trade-off between the processing speed, transmission power consumption, and price. Based on the data load distribution along the path, the nodes in the network are designed in two types called Main Nodes and Sub Nodes to maximize the utilization of the network resource. So the whole data flow starts from the sub nodes of the sensor network, path through the main nodes and be first packed and transmitted to the IHHS.

In the IHHS, local database is designed to manage the data flows and as the uniform data interface between the applications from various service suppliers. Usually the IHHS device is

much more powerful than the sensor nodes, so higher efficiency data compression and visualization can be implemented. The IHHS should also receive data from the service backend e.g. the doctor side or the hospital side. These data could indicate the new schedule of medication, sampling data command, etc. These data are saved into the local database and presented to the user. At the same time compressed or re-packetized data are sent to the service backend.

More complex data analysis and diagnosis tools could be involved in the service backend. Bigger databases should be allocated to manage all the data from the whole system. Here service providers e.g. doctors analyze the uplink data and generate the feedback data. Feedback data will be sent back to the IHHS and presented to the user.

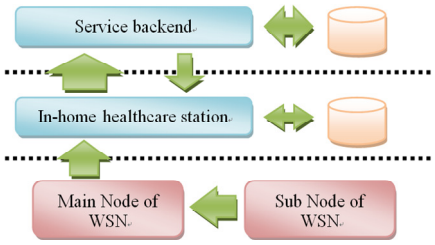


Fig.6. Data flows in the Health-IoT system

B. *Self-contained data formatting*

As mentioned before, the standardized interfaces can improve the interoperability between devices and applications. Complementary approaches are also needed because 1) the number of standardized interfaces is still quite big; 2) it takes time until a few dominative standards are proven in practice; and 3) as the root cause, the ecosystem is open and welcomes new players and new solutions all the time.

As a complementary technical solution, a self-contained data formatting scheme is proposed. As shown in Fig.7, the data between the sensor devices and IHHS, and the IHHS between the service backend are packetized together with concrete descriptions. Each packet has its own header segment. At the beginning of the header segment, there is an optional title to identify the data packets e.g. from which device or patients. And the following bytes are the description bytes. It uses flags to describe the characters of the payload in a packet, which contains the data information.

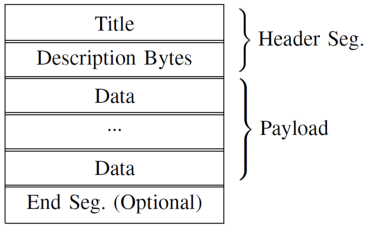


Fig.7. Self-contained data formatting

The descriptions contain all the necessary information to pass and further process the data in the payload such as the packet size, how many samples are contained by this packet, which kind of sensor is used, the node id of the samples, compressing algorithm used for these samples, the compressing step, etc. For example, if the data is from a wearable ECG sensor device, its description segment may contain the manufacturer's information, sample rate, resolution, length, and the compressing/decompressing algorithms if the raw data is compressed.

Because the flag-scheme is used, the description parameters can be updated easily. New features can be integrated and unsupported features can be removed later. After the header segment, there is the data segment. It is the main body of the packet. It contains all the samples data. All the data should match the described structure. At the end of the packet there is an optional end segment. It indicated the end of the packet.

C. *Layered compression*

For most of data compression algorithms, after several compression phases, the data distortion caused by the compressing/decompressing usually gets worse and worse, and the computational complexity gets higher and higher. In the Health-IoT system, from the frontend sensor devices to the remote server, the data content is bigger and bigger, and the device processing speed is faster and faster. So the propose layered compression is to divide the whole data compression process into multiple steps. Based on different processing capacity of the devices, different process load is allocated. After each step, the data size becomes smaller and smaller. This will help to reduce the traffic load and transmission energy consumption of the second half of data path. Taking the advantage of the self-contained data formatting, data packets from one step contains all the information for the next step to decode and further compress the data.

For example, if the compression algorithm in the former step is based on a dictionary, this dictionary can be contained in the description of the packets. Moreover, because the system focuses on healthcare application and the data characteristics are stable, it is possible to use predefined parameters in the compressing algorithm. Saving these values together with the software in different devices, and then there is no need to send the compressing parameters with the data packets. Then along the whole data path, the packet format could keep the same.

VII. THE PROTOTYPING SYSTEM

A. *Application scenario*

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 previous work [14-17]. 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. The iMedBox system is a typical instance of the above terminal design principles.

As shown in Fig.8, 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 Wi-Fi 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.

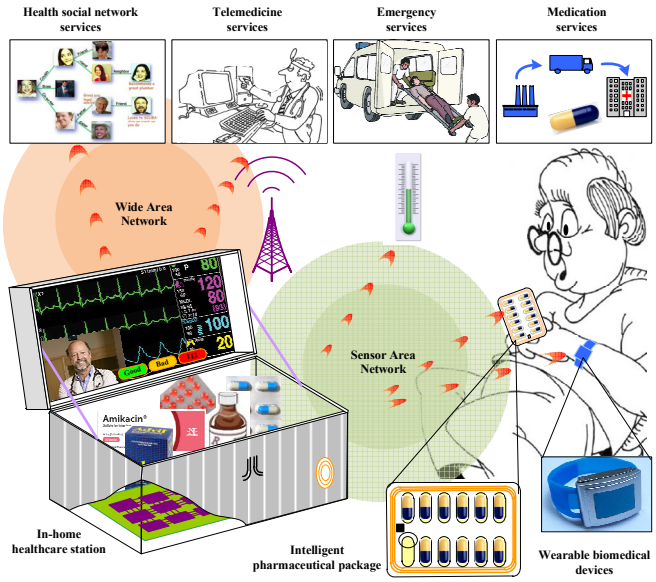


Fig.8. The application scenario of the In-Home Healthcare Station

B. *The iMedBox prototyping system*

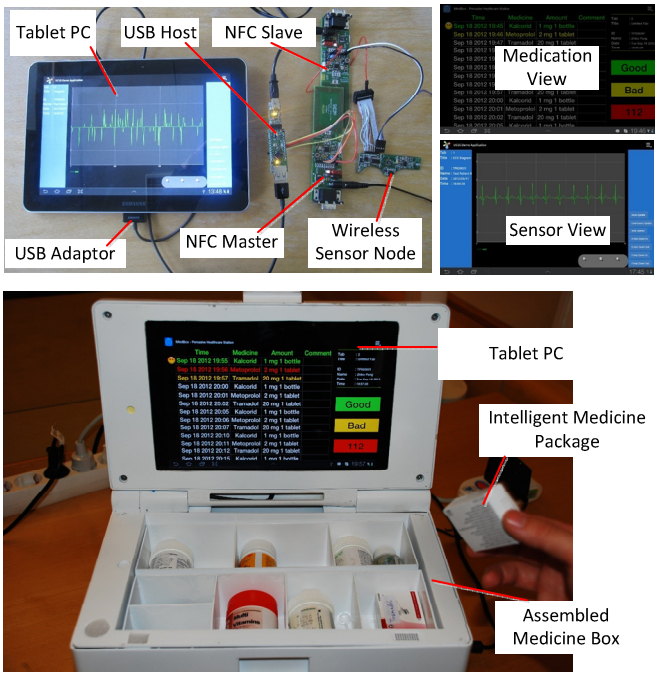


Fig.9. Implementation of iMedBox prototype

A prototyping system of the iMedBox is implemented 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, Wi-Fi and 3G. The operation system is Android 3.1. As shown in Fig.9, 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.

C. *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.

VIII. 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 reconstruction of the traditional healthcare and mobile internet ecosystems. To support this ecosystem, the new ecosystem-driven strategies are applied in all aspects of the development of a Health-IoT solution. As show cases, the design principles or guidelines for standardization efforts, security mechanisms, open-platform-based terminals, and data handling schemes are presented with details. To support fair distribution of benefits among 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. In order to achieve the economy of scale, an open-platform-based IHHS solution is proposed as a universal platform for device and service integration and convergence. Several important design principles are given including common platform based on 3C products, certification of the Health Extension, interoperability and extendibility, convenient and trusted software distribution, standardized and secured EHR handling, efficient service composition, and efficient information integration. Corresponding data handling schemes are designed including the layered data compression and self-contained data formatting.

Finally, 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.

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)

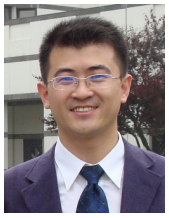
[14] Zhibo Pang, Qiang Chen, Lirong Zheng, "A Pervasive and Preventive Healthcare Solution for Medication Noncompliance and Daily Monitoring", *2nd Inte. Symp. on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2009)*, pp1-6, Nov. 2009

[15] Zhibo Pang, Lirong Zheng, Junzhe Tian, Sharon Kao-Walter, Elena Dubrova , Qiang Chen. "Design of a Terminal Solution for Integration of In-home Healthcare Devices and Services towards the Internet-of-Things", *Enterprise Information Systems*, DOI:10.1080/17517575.2013.776118, April 2013.

[16] Zhibo Pang, Qiang Chen; Junzhe Tian, Lirong Zheng, Elena Dubrova. "Ecosystem Analysis in the Design of Open Platform-based In-Home Healthcare Terminals towards the Internet-of-Things". *International Conference on Advanced Communications Technology (ICACT).* Jan 2013, Pyeongchang, Korea..

[17] Zhibo Pang, Qiang Chen; Lirong Zheng, Elena Dubrova. "An In-home Medication Management Solution Based on Intelligent Packaging and Ubiquitous Sensing". *International Conference on Advanced Communications Technology (ICACT)*. Jan 2013, Pyeongchang, Korea.

[18] Zhibo Pang, "Technologies and Architectures of the Internet-of-Things (IoT) for Health and Well-being", PhD Thesis, Royal Institute of Technology (KTH), Stockholm, Sweden, 2013.



Zhibo Pang received B.Eng. degree in Electronic Engineering from Zhejiang University, Hangzhou, China, in 2002, MBA in Innovation and Growth from University of Turku, Turku, Finland, in 2012, and PhD in Electronic and Computer Systems from the Royal Institute of Technology (KTH), Stockholm, Sweden, in 2013.

He is a research scientist at ABB Corporate Research, Västerås, Sweden. Before joined ABB, he worked as technical manager in semiconductor industry, designing baseband and application processors and turn-key solutions for mobile smart devices. He has 15 patents and over 30 peer-reviewed papers in international journals and conferences. He was awarded the National Great Invention Award by the Ministry of Information Industry of China in 2005, won the First Place Prize of the RFID Nordic EXPO in 2008 and Outstanding Paper Awards in ICACT2013. His current research interests include the Internet-of-Things, wireless sensor network, industrial communication, real time embedded system, enterprise information systems, automation networks, and multicore system-on-chip and network-on-chip. He also works on the business-technology joint research such as business model design, value chain formulation, strategy, and entrepreneurship & intrapreneurship.

Junzhe Tian received B.Eng. degree in Communication Engineering from Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 2010, M.Sc. degree in System-on-Chip Design from Royal Institute of Technology (KTH), Stockholm, Sweden, in 2013. After graduate, he became a Software developer at Excosoft AB Stockholm, Sweden. Currently he is working on design and implementation of Graphical Editing Framework (GEF) and Document Type Definition (DTD) in publishing industry.

Qiang Chen received the Ph.D. degree in electronics from Linköping University, Linköping, Sweden, in 1993.

He was with Ericsson Microelectronics, Stockholm, Sweden, from 1994 to 2002 and became an Ericsson Expert in 2001. He joined Infineon Technology Sweden, Stockholm, in 2003 as a Principal. He has been at Royal Institute of Technology, Stockholm, as a Senior Research Fellow and Project Leader with the Department of Electronic Systems since 2008. He is a Senior Research Scientist with the Department of Electronic Systems and iPack VINN Excellence Center, School of Information and Communication Technology, Royal Institute of Technology. He has published more than 40 international reviewed scientific papers. His current research interests include electronic devices and circuits, wireless sensor network and sensor technology, and printed electronics.