An Intelligent Interactive Home Care System: An MPLS-Based Community Cloud

Farid Shirazi

Ted Rogers School of Management, Ryerson University, Toronto, Canada
f2shiraz@ryerson.ca

Abstract. In recent years, scholarly research on the use of new technology in healthcare has intensified. Some of the main challenges identified in the literature include the integration of dissimilar signaling systems, network barriers such as bandwidth allocation, battery life in wireless devices, the security and privacy protection associated with data transmission using public network and the user friendliness of the systems, among others. The aim of this paper is to address some of the above concerns by introducing a secure, multiplatform network system capable of providing the dynamic bandwidth allocation required for today's home healthcare services. It incorporates a user friendly interface by introducing a unique instrument integrated with the community cloud arrangement to provide a more robust system to address the needs of multiple stakeholders.

Keywords: Cloud Computing, MPLS, ICT, RFID, Virtualization, Smart Sensors, Network Capable Application Processor.

1 Introduction

Despite the fact that cloud computing is a post-Web 2.0 technology, the concept is rooted in earlier technologies such as Grid Computing [1] and distributed computing architecture [2] such as Peer-to-Peer (P2P) architecture. Essentially, cloud computing is a Service Oriented Architecture (SOA) and multiplatform structure, which is integrated with Web 2.0 technology (as its user interface) that provides a layer of abstraction in the form of virtualization.

According to U.S National Institute of Standards and Technology (NIST), cloud computing is a convenient method for gaining on-demand network access to a shared pool of configurable resources (see http://www.nist.gov/itl/cloud/index.cfm). This technology promotes the availability of computing resources (e.g., networks, servers, storage, applications and services) by providing high level abstraction to its users [3]. It allows the customer (users or programs) to request computing resources across the network as needed, anywhere and at any time [4]. This model is composed of five essential characteristics, three service models and four deployment models. The main characteristics of cloud computing are: a) on-demand self-service, b) broad network access in form of support for thin or thick client platforms (e.g., laptops, mobile

S. Yamamoto (Ed.): HIMI/HCII 2013, Part II, LNCS 8017, pp. 207–216, 2013.

phones, iPads, PDAs, servers), c) resource pooling in the form of dynamic allocation of computing resources such as storage, processing, memory, network bandwidth and virtual machines, d) loose coupling structures that provide rapid elasticity or scalability, and e) monitoring services that measure their usage and utilizations [3].

The service model of cloud computing, is composed of three main categories or layers: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). While the SaaS layer provides customers with the capability to use the provider's applications through thin client interfaces such as Web 2.0 based applications, it hides the underlying infrastructure (e.g., server, operating systems, storage and so on) and its location from its ultimate users. Or, as argued by [5], the service oriented characteristic of the cloud abstracts the details of inner implementation. The second layer, or PaaS, supports a set of application programs that interface the cloud applications [5]. It provides a development platform to organizations in the form of programming languages, business logics and management tools for deploying custom designed applications. PaaS hides the implementation details of the underlying infrastructure. Finally, the IaaS layer—also referred to as Hardware as a Service (HaaS)—provides infrastructure support such as processing capabilities, storage, network hardware and connectivity, servers and other computing essentials. While the customers do not manage or control these resources, they may gain limited control of them upon request.

The deployment models of cloud computing include the private cloud (which operates solely for an organization) and the community cloud, which is shared by several organizations by supporting their shared requirements, policies, security concerns and/or compliance considerations. Two other deployment models include the public and hybrid clouds. While the former is a type of cloud offered by a provider to the general public, the latter is a combination of two or more cloud models [3]. The aim of this study is to integrate networked smart sensors into a cloud computing system by providing a user friendly web-based interface to stakeholders (e.g., patients, doctors, nurses, caregivers, pharmacies, central control systems, management, etc.). Providing such a ubiquitous support for home healthcare systems integrated with cloud computing serves as a means to reduce the cost of operations. From the implementation point of view, this study uses an RFID/WiFi converter to extend the signal reach of RIFD devices to a longer distance as well as make it possible for the system to handle RFID data in form of IP packets suitable for transmission over the community cloud. The network infrastructure introduced in this study is designed to securely carry out mission critical data such as patients' health care data with a higher transmission rate while complying with the quality of service offered by the cloud computing and supported by the Next Generation IP Networks.

2 Sensor-Based Home Healthcare System

The world's aging population is growing, so too is the number of people who need post-surgery home care coordination. In addition, post-operative and health care related to children require effective monitoring systems at home. As such there is a need for an effective system that is not only capable of managing the increasing number of

home healthcare service clients but also responds to their needs in a timely manner, regardless of the their location. For example, according to the Health Council of Canada, most seniors in Canada live at home and would like to remain there as long as possible. This includes seniors who are in need of immediate health care support. According to various healthcare reports, the costs of home health care in future are expected to rise relative to the heath sector [6, 7]. As such, Information and Communication Technology (ICT) can be leveraged to contribute to better quality care as well as to help maintain the cost reductions of such a large scale operation.

As noted by [8], healthcare and social welfare systems are being re-engineered globally. Across both the developed and developing world governments are recognizing the need to maintain or reduce costs and to increase the efficiency and effectiveness of healthcare delivery and management. ICTs provide a foundation for transforming supportive apparatuses to meet the complex structure of today's healthcare systems including caring for the patient in the so-called "Hospital without Walls" [8]. As such, the future delivery of healthcare will clearly be predicted on two factors: 1) the provision of ICT infrastructure; and 2) the availability of healthcare and other professionals who are able to utilize such infrastructure [9] as a means of delivering patient care and health promotion in an effective and efficient manner.

Such a holistic approach is best described in the course of its impact on improved healthcare delivery in the form of home care services. This involves an assessment of the role of new technologies in enhancing both efficiency and effectiveness for all stakeholders [9]. The aim of this study is to incorporate wireless network smart sensors through some popular home care applications with a community cloud in a secure manner, as required by today's advanced health arrangements.

2.1 Smart Sensors

In the context of this study, a smart sensor is defined as a low-power, integrated microprocessor circuit that is not only capable of measuring healthcare related tasks with higher precision and accuracy, but it is also capable of communicating wirelessly with other components in an IP-based network. Smart sensors are devices which have been designed using IEEE 1451 (Smart Transducer Interface Standards) family standards for distributed systems integrated with network capable application processor (NCAP). With these, one can access any sensors or actuators in the 1451-based network wirelessly (or wired), independent of the underlying physical NCAP [10].

This paper aims to address some of these concerns by introducing a secure, two-way interactive communications between a centralized community cloud and other stakeholders, including the patients.

2.2 The Home Care Application

The cloud-based home care system of this study is implemented in two main parts: the actual home care system and the MPLS cloud implementation, which will be discussed in the next section.

We consider four major home care applications as a means of implementing an intelligent home care system through the setup of a smart sensor network system in a simulation environment. For simplicity, we limit our application to an RFID-based electrocardiogram (ECG or EKC) for real-time monitoring of electrical and muscular functions of a patient's heart conditions, an RFID-based medication intake box, and two other RFID applications for measuring the patient's blood pressure and body temperature (see Figure 1). This system can be expanded to any other application adhering to IEEE 1451 standards.

At the heart of this system there is a Home Care Controller (HCC) (see Figure 1 part C) which is a virtualized monitoring system connected to the home sensor network and controlled by a centralized home care monitoring system. In this arrangement, smart sensors are implemented as Near Field Communication (NFC) RFID devices composed of sensors with RFID tags, RFID readers and the HCC system.

2.3 The HCC System

The entire home care system is primarily initiated and controlled through a menu driven, user-friendly application. The application running in this system (see Figure 1 part A and B) activates one of the existing RFID readers as desired. The actual activation task, in terms of the signaling processing, is done by a device called a RFID/WiFi (see Figure 1, part C) converter which is wirelessly connected to the controller. As the name indicates, an RFID/WiFi device converts WiFi signals into RFID signals understood by the respective RFID reader and vice versa—it converts RFID signals received from an RFID reader into WiFi signals for further processing in the HCC system. This device is also used as a means of extending the range of RFID signals within a home care unit.

HCC, among others, contains a database for storing collected data locally for further processing. One of the important tasks of such processing is to compare data against preset criteria. For example, if an abnormal activity is detected the system triggers an alert in the form of a warning message displayed on the HCC's monitor, a wave-based buzzer (noise free) is attached to the patient's body or bed and an SMS is sent to the caregiver as well to the centralized monitoring system.

In addition, data stored on a local database can be redirected to the centralized monitoring system for storage into the home care centralized database system (see Figure 1). Further processes might include performing complex calculations and generating web-ready results which can be sent to the respective caregivers via any IP-enabled devices such as an iPhone. As shown in Figure 1 our home care system is a wireless access point/home router connected to cloud by the means of a high speed Internet connection (e.g., cable modem or similar technologies compatible with IEEE 802.11b/g/n, IEEE 802.3/3u (fast Ethernet with auto-negotiation) and IEEE 802.3az (energy efficient Ethernet)) which in turn is connected to IaaS provider's customer edge (CE) router (see also Figure 2). Both HCC and RFID/WiFi are using private IP addresses mainly for security purposes. In addition, two other measures are implemented to protect our home care system. The first measure is to password protect the

system and the second measure is to register the home router's IP address with the provider's CE router so that only authorized IP packets can pass through the CE router. The latter is done through auto-negotiation of WLAN router.

Finally, using collaborative Web 2.0 technology [11], in the case of an emergency, our HCC system is capable not only capable of data sharing with other systems within the community cloud but also it capable of two-way, secure web-based voice and video communication between the patient and/or caregiver and the remote centralized control management system.

2.4 The Home Care Applications

One of the biggest challenges for seniors and other patients resting at home is timely medication intake. Many patients forget to take their medication and cannot recall or remember when, how many or what pills to take, which may lead to complications and health issues [12]. The home care system of this study offers a medication box, equipped with small drawers. Attached to the medication box there is an RFID reader that receives signals from sensors attached to each compartment of the box with a sensing panel door. When the panel door for the assigned daily medication is opened and the pills are taken, a green signal is sent to the HCC controller through the reader; based on the preset criteria, an alert, as described above, is sent out.

An RFID-based sensing blood pressure device is attached to patient's wrist. The RFID reader sends the collected to our HCC via the RFID/WiFi converter. The results will be saved in a local database for further processing. In the case of an emergency, an alert will be sent to the caregiver and other stakeholders. In the same manner the patient's body temperature can be measured (via gastrointestinal, forehead, oral, aural means, etc.) so that the RFID temperature reader receives signals from the temperature sensors and this information can redirect relevant data to the HCC system as described above. Heart disease is one of the most important areas in terms of citizens' health and the cost of operation it implies. A Holter monitoring system was selected for the purpose of recording a patient's ECG (or EKG). The Holter system is essentially an RFID-based ECG monitoring system in which the electrical sensing recorders are attached to patient's body and then the collected data is read by an NFC reader. The process of collecting electrical signal is initiated by the HCC system. Like other RFID measuring equipment, the accuracy of the collected data is a crucial step in providing proper healthcare advice and services. In the case of ECG applications, the sampling rate of electrical signals is the most important factor regarding the quality of waveform data. In addition, the network infrastructure should support the quality of service and reliability of data transmitted over the network to a remote centralized monitoring system. The network should also be able to support the bandwidth required for this purpose since real-time ECG data collection demands significant bandwidth. Finally, the speed of the network should be fast enough to support ECG palpitations so that in the case of an emergency, an immediate alert could be sent to the caregiver.

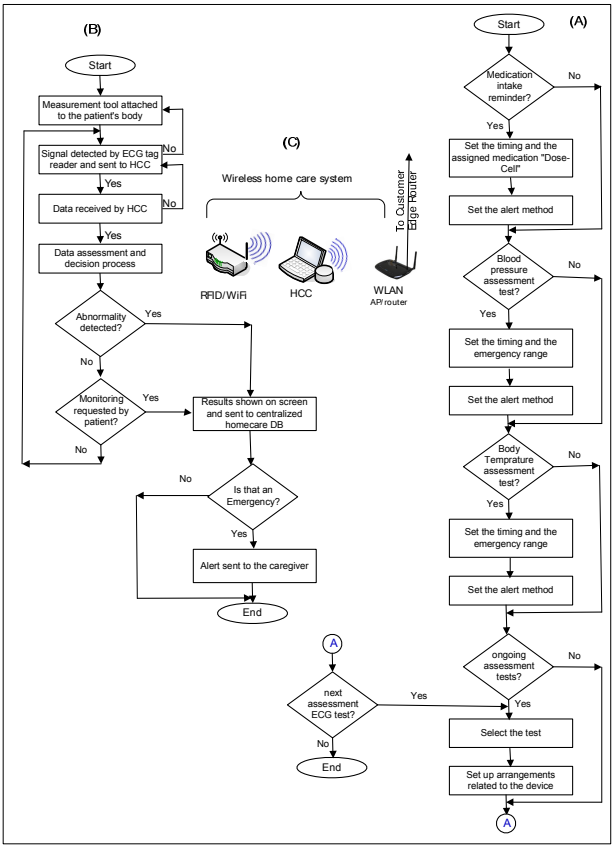

Fig. 1. The Home care controller system

3 MPLS and the Community Cloud

3.1 Network Virtualization

Virtualization is often anchored with cloud computing regardless of its models of implementation (e.g., public, private, community or hybrid cloud). In the context of cloud computing, virtualization is the ability to provide multi-tenant logical cloud services resources from multiple and different physical resources. Virtualization can be implemented at the infrastructural, platform, or software levels. It is often underpinned by the ability to provide a layer of abstraction via the grouping of physical resources to reduce costs and to form a cloud. It can exist in parts or throughout the entire IT stack from server, storage, and service to network virtualization [14] suitable for sensitive data transmission as our home care system. This study implements a type of network virtualization by deploying virtual routing and forwarding (VRF) commonly used in Multi-Protocol Label Switching (MPLS) which allows multiple instances of routing tables to coexist within the same router [14].

3.2 MPLS Cloud

MPLS is a tunneling protocol for secure real-time data transmission over a public network. Mechanisms used in this arrangement increase network security by eliminating the need for encryption and authentication [14]. MPLS offers advanced security features suitable for our home care model. These features include network speed, traffic engineering, quality of service (QoS), Virtual Private Network (VPN) and resiliency. Resiliency in an IP network is centered on the MPLS-based [15] cloud in order to achieve fault tolerance against failures of the network nodes (see Figure 2). Other capabilities of this arrangement include its traffic engineering capabilities and the availability of various classes of services (CoS). These services together offer the required QoS as demanded by highly sensitive networks such as those in healthcare.

VPN is implemented by the means of label distribution protocol. The label distribution protocol, as explained by MPLS, has the ability to reserve network resources for traffic flows. This is a particularly important feature for real-time application such as our home care control system. It also speeds up data transmission by the means of label exchange by routers on the path. Traffic engineering is a useful feature for on-demand high quality network traffic. This extended feature offered by MPLS is executed through a protocol known as resource reservation protocol or RSVP (RFC 3473). This feature allows for better control over network traffic, particularly when sudden variations in traffic patterns and heavy load are traversing the network. Three major components of an MPLS network are: Labels, Ingress/Egress routers and core Label Switching Routers (LSRs) called also Provider Edge (PE) routers. Packets entering into an MPLS cloud are assigned labels. These labels are used as a means of packet delivery and they replace the traditional IP address-based packet delivery. In other words, this system hides the path of IP packets traveling within an MPLS cloud.

Figure 2 shows the implementation of the MPLS cloud within our community cloud. As shown in the figure, an Ingress router is directly connected to the router to deliver health data, also called a customer edge (CE) router. A CE router is any legacy non-MPLS IP router such as BGP or OSPF router. IP packets from CE routers enter into an Ingress router. An Ingress router is essentially an LSR router which is placed on the edge of our MPLS cloud. This router selects the best path within an MPLS network. Then it pushes (injects) a label into each packet entered into the MPLS cloud. The labeled packets are then sent to the selected core LSR router(s). The core LSR router then swaps the old label of each packet with a new label. In this arrangement the core LSR routers are label swappers. Swapping is done as a means of increased security. When the packet reaches the other edge of network, it enters into another edge router called an Egress router. The Egress router then pops (removes) the label and delivers the IP packets to the connected CE router (e.g., the router connected to database server). It is important to note that edge routers are capable of both push and pop operations (see figure 2).

As depicted in Figure 2, core SLR routers are connected in a meshed topology to provide multi-path options as a means of fault tolerance and load balancing for routing traffic from source to destination. It is important to note that MPLS is supported by IPv6.

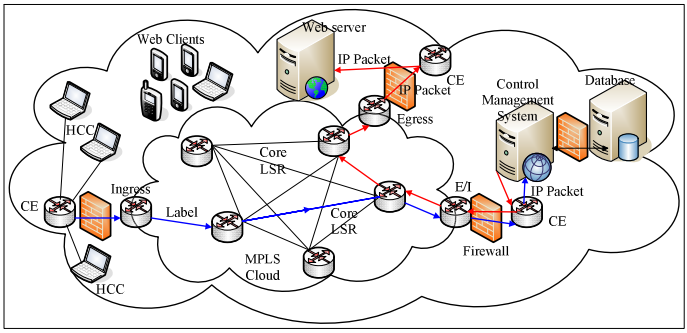

Fig. 2. An MPLS Community Cloud Legend: CE= Customer Edge router, HCC= Home Care Controller, E/I= Egress/Ingress

3.3 Data Processing and Presentation

Our network design, as depicted in the above figure, consists of a community cloud and an inner cloud which is the provider's IaaS MPLS-based backbone.

Data from our home care controller (HCC) systems enters the CE router in the form of IP packets. Firewalls are set up between each CE router and their neighboring Ingress/Egress routers. The reason for such a setup is that while data are secured within the MPLS cloud, they are vulnerable to malicious activities outside this environment. To secure the traffic we implemented firewalls in four main entries as depicted in Figure 2. Home healthcare data, from their collection to the resultant web documents on the clients' IP devices, go through nine distinguished yet interrelated steps as shown in Figure 2. In the first step, the CE router passes data to its nearest Ingress router. This router pushes a label (step 2) on the arriving IP packets and then forwards them to a neighboring core LSR router. After label swapping on the core LSR routers (step 3), packets arrive at the Egress/Ingress (E/I) router. The Egress router removes the label (step 4) and forwards the IP packets to the CE router that is connected to our centralized home care control management system (administrative) which in turn is connected to our centralized backend database server.

Authorized queries are forwarded to the database. In step 5, our database system responds to client queries in XML format packaged into IP datagrams. IP packets are then sent to a CE router connected to our monitoring server and from there they are forwarded to the E/I router. As a receiver, this router is now acting as an Ingress router, which pushes labels into IP packets (step 6). These packets are then forwarded to an LSR core router. The LSR core routers on the path swap labels with new values (step 7). The final destination of XML data within our MPLS cloud is an Egress router. After the pop operation (step 8) of the labels, IP packets are sent to the nearest CE router connected to our web server. This server is a virtualized multi-tenant web server capable of providing support to multiple applications and/or servers as a single system thus providing a more secure and robust topology than a legacy non-virtualized server. One key point in this arrangement is to hide the availability of multiple servers from the outside world [14]. The web server sends collected data in the

form of web documents (step 9) to clients requesting the data by the means of a secure HTTPS protocol. Personal health applications allow their users to store a wide variety of personal health information and data ranging from medical conditions and test results to medications and allergies [9]. In this arrangement, clients are any IP enabled devices with authorized access to healthcare data (e.g., ECG data). The system is also capable of two-way, web-based secure video communication between HCC and the home care control management system.

One of the main drawbacks of the implemented virtualized network is its high demand on WAN link for a real time/on-demand data delivery. In this context, the network virtualization and MPLS are both bandwidth demanding applications not suitable for slow WAN link connections. In addition when the number of HCC systems attached to this system increases the demand on network bandwidth will increase significantly.

4 Conclusion

In this study we presented an intelligent home care service using a centralized monitoring system to incorporate a healthcare system into a community cloud shared by multiple parties. Our innovative home care cloud is a centralized system which offers various controls and alarm mechanisms designed to react responsively in emergencies. Using Web 2.0 technology, the user-friendly interface is capable of mentoring multiple patients simultaneously and reporting their health conditions to doctors, nurses and caregivers, as requested.

The contribution of this study is the implementation of a home care system that is fast and more reliable. It offers a flexible data routing mechanism in the form of traffic engineering, and provides the quality of service required by healthcare applications. It also offers a secure environment via MPLS protocols for transmitting medical records over public infrastructure. Smart sensors implemented in this system use RFID signals incorporated with the advanced features of wireless IP network. We proposed an interactive, menu-driven home care system called HCC in which the application running on this system controls the wireless sensor network and redirects information to a centralized location for further processes. In addition, the outcome of such processes can be sent simultaneously to multiple stakeholders if required. Finally, our system uses the virtualization features of cloud computing to dynamically expand the home care nodes to help reduce the cost of public healthcare systems. Another advantage of using an MPLS-based community cloud is its ability to integrate IPv6. However, the limitation of this system is its dependency on medical devices attached to wireless sensor networks. Improper installation of RFID devices and/or problems with faulty signals may cause problems when locating the root of functional problem. Therefore, testing the medical equipment is a vital task in the successful implementation of this system. It is also required that caregivers have appropriate ICT skills and training when engaging with the system's interfaces.

Acknowledgement. The author appreciates the assistance of Parisa Lak. Parisa's knowledge in the field of healthcare management has greatly contributed to this study.

References

1. Foster, I., Zhao, Y., Raicu, I., Lu, S.: Cloud Computing and Grid Computing 360-Degree Compared. In: IEEE Grid Computing Environments (GCE 2008), pp. 1–10 (2008)
2. Zhang, Z., Zhang, X.: Realization of Open cloud Computing Federation Based on Mobile Agent. In: 2009 IEEE International Conference on Intelligent Computing and Intelligent Systems, pp. 642–646 (2009)
3. Mell, P., Grance, T.: The NIST Definition of Cloud Computing (2009), http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf
4. Yan, S., An, G.H.: Software Engineering Meets Services and Cloud Computing. IEEE Computer Society (October 2011)
5. Gong, C., Liu, J., Zhang, Q., Chen, H., Gong, Z.: The Characteristics of Cloud Computing. In: IEEE 39th International Conference on Parallel Processing Workshops, pp. 275–279 (2010)
6. Coyte, C.P., McKeever, P.: Home Care in Canada: Passing the Buck. Canadian Journal of Nursing Research 33(2), 11–25 (2001)
7. Tarricone, R., Tsouros, D.A.: Home Care in Europe. The World Health Organization Publication, Milan (2008)
8. Carson, E.R., Cramp, D.G., Hicks, R.W.: Hospital without walls. Computer Methods Program in Biomedicine 64, 153–242 (2001)
9. Cramp, D.G., Carson, E.R.: A model-based framework for assessing the value of ICT-driven healthcare deliver. Health Informatic Journal 7, 90–95 (2001)
10. NIST, Brief Description of the Family of IEEE 1451 Standards (2009), http://www.nist.gov/el/isd/ieee/1451family.cfm; See also: IEEE 1451 Family of Smart Transducer Interface Standards, http://grouper.ieee.org/groups/1451/0/body%20frame_files/Family-of-1451_handout.htm
11. O'Gradya, L., Wathenb, C.N., Charnaw-Burgerc, J., Betel, L., Shachakc, A., Luked, R., Hockemac, S., Jadadc, A.R.: The use of tags and tag clouds to discern credible content in online health message forums. International Journal of Medical Informatics 81, 36–44 (2012)
12. Schoen, C., Osborn, R., How, S., Michelle, M.D., Peugh, J.: In Chronic Condition: Experiences of Patients With Complex Health Care Needs, in Eight Countries. Health Affairs 28(1), 1–16 (2009)
13. Kaplan, B.: Evaluating informatics applications—clinical decision support systems literature review. International Journal of Medical Informatics 64, 15–37 (2001)
14. Josyula, V., Orr, M., Page, G.: Cloud Computing: Automating the Virtualized Data Center. Cisco Press, Indianapolis (2012)
15. Autenrieth, A.: Engineering end-to-end IP resilience using resilience-differentiated QoS. IEEE Communications Magazine 40(10), 50–57 (2002)