e-Healthcare Cloud-Enabling Characteristics, Challenges and Adaptation Solutions

Wei Liu[1] and Eun K. Park[2]
[1] Georgia Gwinnett College, Lawrenceville, GA 30043, USA
[2] California State University, Chico, CA 95929, USA
Email: wliu@ggc.edu; ekpark@csuchico.edu

Abstract—This paper focuses on the e-Healthcare application cloud-enabling characteristics as we uncover the close proximity of the new e-Healthcare architecture and the cloud environment. However there are still challenges in adaptation of a pure cloud solution for digital e-Healthcare. This paper documents those similar characteristics and the new challenges. It also introduces our adaptation architecture design for e-Healthcare Cloud Computing and Networking Solutions.

Index Terms—Cloud technology, Cloud process, Cloud-enabling e-Healthcare, e-Healthcare adaptation architecture, e-Healthcare cloud solution

I. Introduction

We define Cloud Computing, in the context of e-Healthcare applications, as an application-oriented and service-based infrastructure where Health-IT resources are pooled, allowing services to be widely deployed or rapidly shared in response to changing healthcare business and regulatory requirements.

The e-Healthcare cloud is illustrated in the Fig. 1 below. From the user point of view, the internal resources and application processes are transparent and the users are mainly concerned with the standardized healthcare records and the familiar health information technology capabilities.

An e-Healthcare cloud includes the underlying technology, the operational process, and the new commercial utility paradigm. As the world is increasingly moving away from development-centric view to one that is focused on applications, information, and people thus more towards to the new paradigm of cloud computing.

Unlike information technology providers of Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), Network-as-a-Service (NaaS) and others as-a-Service endeavors where the main focus is on cost reduction, speeding-up life cycles and scalability for existing applications, we extend the cloud paradigm to serve emerging global demands in digital health care applications.

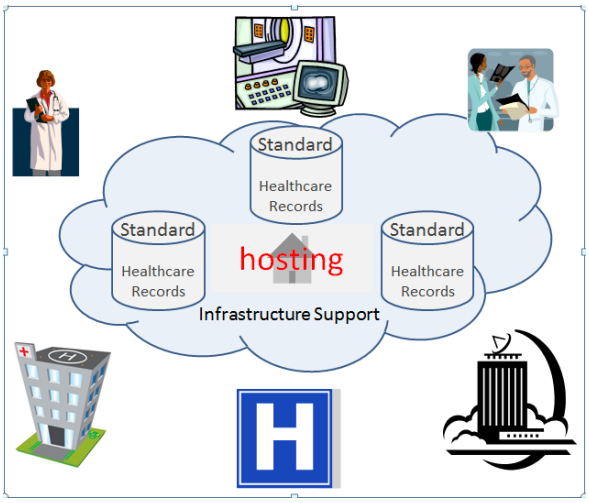

Figure 1. e-Healthcare capabilities as cloud computing applications.

We take it into consideration to incorporate regulatory mandates, service managements, handheld on-demand access, quality-of-service accounting, and system interconnection requirements. Our work also covers security of the cloud infrastructure that enables multi-party participation, allows variable visibility into selective parts of data, and guarantees end-to-end security control. From the application standpoint, the cloud network service infrastructure shall become enablers to revolutionize the roles and responsibility of the healthcare professionals as well as e-Healthcare consumers. Our paper further addresses next generation communication service clouds that support pervasive healthcare applications together with additional operational management capabilities. We extend beyond a platform level solution for rapid communication session service creation by incorporating existing as well as new healthcare information network and operational capabilities.

This paper is organized as follows. Section II describes our analysis of the e-Healthcare computing characteristics and the close proximity of the cloud paradigm. In section III, we describe the major challenges in interconnection service, security service, operational management, as well as the architecture of e-Healthcare cloud service access environment. In section IV, we include a state of the art adaptation and operational architecture in governing diverse cloud providers whether they are offering public

Manuscript received December 31, 2012; revised October 10, 2013
Corresponding author email: wliu@ggc.edu
doi:10.12720/jcm.8.10.612-619

or external private clouds. Finally in section V, we conclude with a summary of the paper with additional recommendations for further advancement.

This paper is related to our previous work in the e-Healthcare infrastructure services, but with a major shift into the cloud paradigm. In [1]-[2], we researched the integrated infrastructure solutions and security challenges in e-Healthcare. In [3]-[5], we developed interconnection architectures as well as operational solution, and we explored the new service creation paradigms. Other works that are related to our discussions include [6] that concerns the adoption of cloud technology and [7]-[8] with a focus on security challenges. The various prior solution foundations can be found in [9]-[18] where interested readers can also find e-Healthcare background information, service layer management and additional success stories or lessons learned from various industry parties and their project reports.

II. E-HEALTHCARE CLOUD CHARACTERISTICS

A. Technology

The essential characteristics are mainly in the technological areas. The decomposed elements are summarized in the Table I .

TABLE I: E-HEALTH CLOUD UNDERLYING TECHNOLOGIES

characteristics	Description
Resource	Computer nodes, Storage nodes, Management nodes, Network nodes.
Virtualizations	Virtualization modules, automatic scheduling, on-demand provisioning.
Access	PC, Phone, Server, any time, any device and Location transparency.
Scalability	Meet SLA (service level agreement), Redundant capacity to meet spike.
Security	Centralized data with security, Centralized physical infrastructure.
Operation	A centralized, automated, and integrated set of tools to provide consistent management for the underlying physical and virtual environments.

The main characteristics of a cloud are to pool the resources together and to deliver application services on-demand with economical scale.

The fundamental feature of e-Healthcare cloud should be in rapid provisioning and interconnection of resources, including electronic patient and medical records of medical history, allergies, vaccinations, appointments, and invoices as well as inquiry; clinical supports and medications with processing for prescription, transcription, dispensing, and prescription administration.

As these resources require large number of system nodes listed in the above table, the technical characteristics to achieve rapid distribution of resources can be found in solutions such as rapid node/port resolutions, resource distributions and provisioning, service description, location and access controls.

Delivery with service level agreement will become the hall mark of cloud services. The Quality-of-Service (QoS) technology in the context of e-Healthcare has been discussed in [3], with the key technology of formulation and guarantees in end-to-end service delivery.

Other cloud standards in virtualization can follow the best of breed in the market where data center consolidation and virtualization have become commodity. Common technology characteristics include

- OS-level virtualization and user-space isolation
- Full virtualization with an unmodified "guest" OS to be run in isolation
- Hardware-assisted virtualization with virtual machines and address space virtualization
- Paravirtualization with special APIs to modify "guest" OS.

Another common technical feature is concerning scalability and reliability. While user demands usually are averaged out, a total cloud solution has to scale to handle service peaks. The key technology is to aggregate the static Service-Level-Agreements and plan for overall capacity [4]-[5]. Access should be available anytime, anywhere and to all authorized users. If mobile devices are allowed to access the medical records, they can contain large amounts of data and computing power and are easy to connect to the Internet and other devices.

Data encryption and clear policies and processes for encryption are vital to technology features. The gold standard encryption is the Advanced Encryption Standard at its highest level of security of 256 bits (a.k.a. AES-256). Also, key management must be tightly controlled.

Operational features covering replication and redundancy with multiple copies of files and messages in multiple locations can help guard against accidental loss or corruption. Current standard technology can reliably retrieve the correct version, provide availability in the face of a failure at any individual data center, and synchronize the versions that exist at multiple sites.

Other operational management capabilities include auditing and reports. Management needs insight into who has access to resources, which application is using those resources, and what changes have been made. The best systems also provide customizable versioning to make it possible to quickly and easily reverse damages from undesirable changes or deletions.

B. Process

Agility is the key feature required by the emerging e-Healthcare services where doctors, hospitals, clinics, insurance, pharmacies all want all of patient medical

prescription data conveniently and reliably accessible no matter where or how it is stored, no matter what kind of applications they're using to access files, and no matter what type of devices are at their fingertips—a smartphone, a tablet, a laptop, or a desktop. They want to be able to work and serve their patients from anywhere at any time.

On the other hand, there are regulatory requirements [9]-[11] on strict security requirements, which cause additional layer of requirements to roll out e-Healthcare service in a shared cloud environment. But to enhance efficiency, the providers and associated entities want to share these medical records and related services without cumbersome access controls and login procedures.

The cloud infrastructure can deliver the agility that e-Health users desire with inherent security capabilities that the security IT requires, and in doing so it can preclude the need for "backdoor IT" where health IT users or others create their own workarounds to avoid cumbersome security requirements.

An additional process shift in the cloud is moving capital expenditures into operational costs. A cloud offering is a pay-as-you-go service, so there are no new capital expenditures for servers, storage systems, and VPN connections; there are no software upgrades and support costs; there is no need to hire and train new system administrators. The medical providers and the patients mainly want to focus on the strategic roll-out of e-Healthcare services and so they want decreased IT cost and risk.

From the healthcare professional's view, the cloud services are automatically provisioned and deployed, with month-by-month terms available. The Health IT process no longer risks the expensive upfront investment of the usual hardware and software solutions. The cloud service also typically works with a multitude of devices, scales on demand to accommodate growth or spikes in usage, and is accessible 24/7 virtually from anywhere via internet.

The cloud model can also give companies the ability to leverage resources they already have—including both physical infrastructure such as servers and storage systems as well as existing user credentials and security-related processes. This means that IT can extract even more value from these resources by cloud enabling them rather than forcing a "rip-and-replace" migration that increases risk across the board. At the same time, the move to the cloud model can unburden the IT department of the need to develop and maintain expertise in every facet of data security. The key elements of security are left to specialists.

The e-healthcare cloud model requires a change in IT processes, moving from a reactive, tool-centric model of resource management to a proactive model that uses streamlined processes and automation. To achieve this vision, e-Healthcare IT services must shift its focus into e-Healthcare service composition, service discovery, business workflow and new organization models making the processes both scalable and flexible.

C. *e-Healthcare as Shared Commercial Service*

To implement a new e-Healthcare cloud solution process, the stake holders (providers, insurance and other business associates) [10]-[11] may need to adopt a shared service paradigm.

A number of commercial paradigms are possible for cloud computing services. To ensure better control of the cloud operation, a private infrastructure is operated solely for a single organization. It may be managed by the organization or a third party and the infrastructure may be located on-or-off premises. While the organization does not need to physically own or operate all the assets, the key idea is that a shared pool of computing resources can be rapidly provisioned, dynamically allocated and operated for the benefit of a single organization.

When organizations use public clouds for private business benefits, they do not control how those cloud services are operated, accessed or secured. While the key elements of security are left to specialists, the e-Healthcare services also retain business rules available in legacy implementations. More importantly, the business rules should specify end-to-end, lifecycle control over where, when and how the business data are created; to whom and where information may flow; and ultimate archive or clear out responsibilities.

If a healthcare service provider needs to leverage its own health IT infrastructure, one may adopt a Hybrid Cloud, where the cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain as unique entities but are bound together by a standardized or proprietary technology that enables data and application portability (e.g., cloud scaling for load-balancing between clouds and/or via distribution of functionality.

III. Cloud Challenges With Digital e-Healthcare

There are new challenges raised by the unique requirements of the e-Healthcare industry for using cloud services by e-Healthcare providers:

- Regulatory
- Security
- Access adaptation
- Inter-cloud connectivity
- Resource distribution.

A. *Regulatory Constraints*

One of the greatest challenges for organizations leveraging cloud environments is demonstrating policy compliance.

For e-Healthcare processes and sensitive EHR (Electronic Health Records) data, it is absolutely essential for organizations to be able to verify for themselves that the underlying cloud infrastructure is secure. The use of

virtual machines adds further complexity into the mix, since creating an identity for an individual virtual machine and tracking that virtual machine from creation to deletion can be challenging even for the most mature virtualized environments. Proving that the physical and virtual infrastructures of the cloud can be trusted becomes even more difficult when those infrastructure components are wholly owned and managed by external service providers. Cloud providers must be able to demonstrate that they have tested and can ensure that privileged user access is controlled and monitored.

Additional regulatory constraints also define the roles of providers in digital healthcare as well as mandatory timelines in applications deployment. For example, the Health Insurance Portability and Accountability Act (HIPAA) and the Personal Information Protection and Electronic Documents Act (PIPEDA) require health data be processed in certain prescribed means. If an entity (user) is covered by the regulatory acts, the business associates (vendors) have to demonstrate that their cloud services also meet the requirements.

B. Security Constraints

According to the Cloud Security Alliance [8], the top threats to Cloud Computing include:

- Abuse and nefarious use of cloud computing
- Malicious insiders
- Insecure interfaces and APIs
- Account or service hijacking

In addition, there are e-Healthcare specific security requirements that may be magnified by the cloud scale. As such, an overall security framework will further tighten security requirements [2].

- Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities and impacts;
- Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable;
- Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis;
- Increase the efficiency of security operations in transmitting and processing of electronic medical records, personal healthcare records, and patient billing records, as well as public health alerts, across many parties with varying security, privacy and trust levels.

C. Access Adaptation

The ease of access and flexible configuration for the users are the main deciding factors in roll out rates and acceptance by the medical professional and by the patient consumers.

Because of some of the new services are mandatory with a regulatory timeline (e.g., IDC-10 release in converting to new international disease coding procedures), the clinical IT services to support those conversions should be seamless and continuously evolving.

Access models also encounter challenges in leveraging private resources (such as patient records). For example, to ensure security, e-Healthcare cloud systems may provide exclusive private resources for users at certain costs. The access adaptation may be deferred until rigorous authorization has been conducted. Even then, additional orchestration rules may impose operational constraints. For example, a business associate may not have the same level of access as a business entity in current healthcare reform requirements.

D. Inter-Cloud Interconnectivity

Application programming interface (API) accessibility to software that enables machines to interact with cloud software in the same way the user interface facilitates interactions between humans and computers. Cloud computing systems typically use REST-based APIs. REST (or REpresentational State Transfer) is a style of software architecture to follow the web paradigm.

But for e-Healthcare cloud services, there are no well-defined REST-APIs existing for current practices and emerging services. The only mechanism that can be easily adopted is the data format as well as emerging workflow services. The interconnection of e-Healthcare services should also solve the issue of extensibility (when a provider needs instance augmentation of additional e-Healthcare applications or new service capability).

E. Resource Distribution

Existing health IT infrastructure already contains most (if not all) of the resources to lay the foundation of e-Healthcare capabilities. Those existing IT resources supply the elements for patient IDs, credentials, appointment, diagnostic, subscribe, remote monitoring, medical and health records as well as other healthcare business tasks. The challenge is to leverage those resources already out there by incorporating or cloud-enabling them in order to extract even more values from these resources.

The cloud-enabling challenge is to distribute the resources in an optimal way across intra- and inter-clouds. The operational process also requires auto-provisioning and high degree of availability so that they can be scale-up in real time to meet the cloud-based e-Healthcare application users.

IV. Cloud Architecture Adaptation Solutions

So far, there are no “pure” cloud services that meet all the challenges raised by the unique requirements of the e-Healthcare industry. We designed an adaptation-

architecture to converge the Health IT solutions into a cloud paradigm (as shown in Fig. 2 below).

The key in e-Healthcare access and cloud convergence will be in application hosting, security service layer, interconnection (inter-cloud) management and cloud service access.

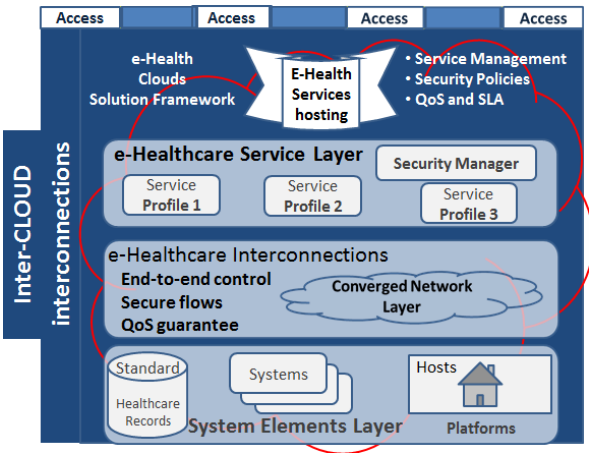

Figure 2. Cloud adaptation architecture solutions

A. Application Hosting

The e-Healthcare Cloud Service model eventually is defined by the underlying e-Healthcare domain capabilities, including the following resources being distributed inside a cloud.

- Personnel-support resources can gather, store and deliver medical information (e.g., electronic patient and medical records) to patients and doctors remotely, including medical history, allergies, vaccinations, appointments, and invoices as well as inquiry supports.
- Clinical-support resources can gather, store and retrieve patient medical information for use internally by physicians and healthcare workers delivering services at the point of care. The admin and supervisory personnel can have access to backend processing of resources, insurance claims and billings.
- Medication processing resources will allow remote information processing for prescription, transcription, dispensing, and medication administration. The systems involved are order entries with validation of drug-to-drug interactions, allergy and dose checks, pharmacy database access, decision modules, as well as record keeping applications.
- Research-support resources gather, store and analyze patient medical information for use by researchers and for government (CDC or Center of Disease Control) reporting. The research systems also support new scientific discoveries in seeking better disease management regimes, and monitoring public health.

In addition, application management (supporting) capabilities have to include Service Ordering, Status, Mediation or Request/Replies, Usages Billing, Problem Resolution, Performance, and ultimately User Supports.

B. Cloud Interconnection Services

To overcome the lack of e-Healthcare APIs in current market places, a converged interconnection service layer [1], [4] is adopted in place with uniform service format and data adaptation capabilities. The uniform format is to simplify implementations. The access gateway can leverage two or more clouds. As such, the access-gateway concept is further extended into interconnection of clouds.

In the interconnection setting, while each cloud is supplying the resources (as a service) via an e-Health gateway, it further consumes the capabilities of another cloud. The consumed services could be a new health treatment capability in scaling up the business offerings, and the consumed resources could offer the same medical data processing capability in order to enhance availability or performance of a servicing cloud. End-to-end control, security policies and QoS guarantees are the key building blocks of the converged networking services [1] in order to support inter-cloud interconnections.

C. Security Service Layer

Additional security solutions in e-Healthcare settings are formulated [2] beyond traditional data networking services. The (security) policies are in place before any external accesses to the cloud services are granted. When multiple entities are participating in a coordinated e-Healthcare process, the security associations will be managed by a Security Service Manager to coordinate the communicating groups.

An implementation of a security manager must maintain three databases:

1) Security policy collections

The Security Policy Database specifies what security services are to be offered to the IP traffic, with rules such as types of source/destination and so on. It contains an ordered list of policy entries. These entries might specify that some traffic must bypass the adaptive security flow processing, some must be discarded, and the rest must be processed by the security manager modules.

2) Security association flows

The Security Association Database contains parameter information about each e-Healthcare Application Flows, such as e-Healthcare routing algorithms and keys, protocol mode, and flow-level lifetime. For outbound processing, the selective encryption scheme has to be applied. For inbound processing, the Policy Collection is consulted to determine how the packet must be processed. If necessary, each provider's internal security module is notified to log the processing activities.

3) Distributed logs

Once a secure e-Healthcare association is established, both end points may invite others to participate in a shared care processing. Therefore, the related processing logs can no longer be kept in separate repositories (possibly even belonging to different clouds). Our

solution requires that a logging mechanism be maintained in the cloud(s) that have access to both Identity/Certificate registration information as well as its own log repositories.

D. Access Gateway

Once e-Healthcare resources are pooled together to form a cloud, new service-capabilities are then supplied and published via an access gateway to the e-Healthcare capabilities.

The concept of gateway is to map the technology of virtualization into the application layer logic, where services are standardized with a complete service directory that can be discovered. E-Health services are submitted as orders, with automatic status tracking and confirmation.

Usually the user devices contain very little built-in security, mostly with remote wipe in the event the device is lost or stolen, or a PIN (in addition to their normal password) as well as access policy checks. As the security is a priority during access, it was also discussed in the security service subsection above.

The Access Gateways allow host-to-host, application-to-applications or user access from doctors, patients, clinical supports, insurance and government agencies. During the gateway operational phases, dynamic Quality-of-Service drives automatic access adaptation by feeding real-time parameters into operational management center for automatic provisioning of new resources.

The overall components of the various aspects (in access, security management, interconnection, and application hosting) become the core of our cloud adaptation architecture. To further validate our architecture solutions, we have also developed a deployment acceptance plan to enable field operations.

V. Solution Validation Plan

Our validation plan shall cover the aspects of practical deployment of the e-Health cloud architecture solutions.

A. Validation of e-Healthcare Cloud Solution Scope

The starting point for validating the solution scope is to revisit set of objectives for e-Healthcare solutions. The quantifiable aspects of objectives usually identify the boundary points and the scope for validation plan.

This architecture solution covers all application resources (i.e., the system elements of clinical, medical and patient supports), the networking resources and interconnection gateways, as well as those services identified in Section IV. The aggregation of all resources and parts into a whole solution has to conform to the overall e-Healthcare solution objectives.

B. Validation of Cloud Service Providers

Cloud e-Healthcare is such a huge topic and will eventually involve various platform or application service providers. Our plans cover designing a specific validation so that we can accomplish the validation of a realistic "cloud" e-Healthcare solution. Here we will take into consideration of the partnership organizations in the network, the selected application systems and the privacy policy from each participant(s).

C. Validation of Technology Infrastructure

Our plan validates the cloud technology infrastructure including software, hardware, and network. We can determine whether the participant's existing information technology infrastructure meets the requirements by validating the interconnection, security and QoS components of our solution as follows.

A secure network connecting to the cloud is required for transmission of clinical data. Additional secure flows are setup to validate the differential security aspects of Data Interoperability.

Different flows have to be performed and validated, between the lab and the pharmacy in a hospital, as well as across institutions, between hospitals and government agencies. Validation plans have to be customized for participating "clouds" partners.

Adaptation connections may be used to enable the "service centers" and "operational centers" in our overall e-Healthcare solutions, so that the architecture can be validated before any costly centers are built.

Validation of QoS can be achieved via statistical data from the "network connections" as a part of the operational plan. Once we collected enough QoS data, we may identify any networking or cloud bottlenecks. Future performance plan will identify the steps to tune for optimal performance.

Configuring the interconnection may be necessary for specific deployments. While we believe the architecture solution principle is sound in our paper, we will work with detail systems to fine tune their participation into this architecture solution.

Validating live exchanges of e-Healthcare Messages: this activity shall validate data interoperability and collect individual performance data for each message.

Overall architecture validation: Once we complete the detail validation plans, we still need to consolidate the "aggregated" results. As the architecture solution can accommodate additional designs in the future, the architecture has to be validated to be compatible with additional emerging e-Healthcare standards.

VI. Summary And Future Research

This paper covers the integrated aspects of cloud computing applications for a global e-Healthcare solution. The benefits of this design approach include adaptation of critical health information technology into a cloud environment while allowing long term evolution of interconnected cloud solutions for e-Healthcare applications.

The overall contributions of our research are in our innovative e-Healthcare application hosting, cloud service access adaptations and interconnection architecture. Additional new features are explored in our security and operational designs to overcome the new e-Healthcare cloud computing challenges and regulatory requirements such as security policies, access adaptors with SLA and QoS constraints, inter-cloud connectivity, and resource distribution into cloud hosting applications.

The key contribution of our paper is our global consideration of macro level issues that have never been systematically addressed in current national trials or regional planning programs. We can now provide the solution framework architecture to guide the Interoperability, the Security, and the QoS management.

1). The interoperability network convergence layers solution is our main contribution and can be readily applied to the inter-CLOUD environments.
2). The security processing will become a new algorithm once the solutions in paper [2] are standardized and applied to the cloud interconnection environment as described in this paper.
3). In the design of our operational methodology, we have applied well proven approaches in traditional telecom domains [3], [17]; and for the first time it was applied to a Cloud computing service environment for QoS management.
4). In applying our innovative e-Healthcare interconnection solutions into the clouding computing environment, we were able to contribute to the research community with the new characteristics and issues as reported in this paper.
5). Additional innovative aspects are our security and operational designs to overcome the new e-Healthcare cloud computing challenges and regulatory requirements with security and QoS constraints, inter-cloud connectivity, and resource distribution into cloud hosting applications.

In the future, we also plan to conduct research in the areas of emerging new service platforms and integration models so that a truly global e-Healthcare cloud (or federated clouds) can become a reality to serve the daily needs of the world.

REFERENCES

[1] W. Liu, E. K. Park, and U. Krieger, "e-Health interconnection infrastructure challenges and solutions overview," in *Proc. 14th IEEE International Conference on e-Health Networking, Application & Services*, Beijing, China, October 2012.

[2] W. Liu and E. K. Park, "e-Healthcare security solution framework," in *Proc. IEEE International Conference on Computer Communication Networks, MobiPST*, Munich, Germany, August 2012.

[3] W. Liu and E. K. Park, "e-Health service characteristics and qos guarantee," in *Proc. IEEE International Conference on Computer Communication Networks, Workshop on Context-aware QoS Provisioning and Management for Emerging Networks, Applications and Services*, Maui, HI, August 2011.

[4] W. Liu and E. K. Park, "Emerging platform for healthcare it services," in *Proc. IEEE International Conference on Computer Communication Networks, WiMAN Workshop*, Zurich, Switzerland, August 2010.

[5] W. Liu, "Digital Health Care (DHC) information technology infrastructure framework," in *Proc. IEEE Consumer Communications Network Conference*, Las Vegas, USA, January 2010.

[6] L. Chung, "Securing data in the cloud: 10 critical questions to ask your cloud provider," Syncplicity White Paper, 2012.

[7] Beyond Trust Inc., "Securing privilege delegation in public and private cloud computing infrastructure," Beyond Trust Software White Paper, 2011.

[8] Cloud Security Alliance, "Top threats to cloud computing v1.0," March 2010.

[9] S. D. Cannoy and A. F. Salam, "A framework for health care information assurance policy and compliance," *Communications of the ACM*, vol. 53, no. 3, March 2010.

[10] U.S. Department of HHS, "Health information technology: Initial set of standards, implementation specifications, and certification criteria for electronic health record technology," January 2010.

[11] U.S. Committees on Energy and Commerce, Ways and Means, and Science and Technology, "Title IV - Health information technology for economic and clinical health act," January 16, 2009.

[12] IT World. (August 2009). [Online]. Available: http://www.itworld.com/networking/75306/us-pledges-12-billion-digital-health-networks

[13] U.S. Department of Health & Human Services. National health information network. [Online]. Available: http://healthIT.hhs.gov.

[14] M. Ballard, "Accenture: NHS failure is 'track record for success'," posted in *IT Channel*, September 28, 2006.

[15] J. Walker, *et al.*. (January 2005). "The value of healthcare information exchange," *Health Affairs*, [Online]. Available: http://content.healthaffairs.org

[16] W. Liu, "Integration of wireless access and wireline networks: OAM&P architecture with itu-tml technologies," IEC Broadband Wireless Report, International Engineering Consortium, December 2004.

[17] ANSI, American National Standard Institute, "OAM&P information model and services for interfaces between operations systems across jurisdictional boundaries to support configuration management customer account record exchange," technical editors W. Liu and J. Ng from T1M1 Standard Committee, 1999.

[18] NRC (National Research Council), "For the record: protecting electronic health information," National Academy Press, Washington, DC, 1997.

Dr. Wei Liu received his Ph.D. from Georgia Institute of Technology in Atlanta, Georgia USA. He is a founding IT faculty member at the GGC School of Science & Technology in Lawrenceville GA. He researched and taught TCP/IP networks in

the University of Maryland prior to his 10 (plus) years of technology leadership career in the industry, where he participated in a number of network transformation projects and service development integration programs. He also provided thought leadership for infrastructure development initiatives at major Technology Labs. He received awards for his contributions to industry and ANSI standards development. He coauthored with IBM the well-known book of "TCP/IP Tutorials and Technical Overview" with 1,000 pages of descriptions of Internet-related protocols and advanced applications back in 2006. Currently, he is investigating new infrastructure opportunities (in e-Health, government, military, network and service convergence, security, and other big data applications) that can lead to future offerings and new IT capabilities.

Dr. Eun K. Park received the Ph.D degree in Computer Science from the Northwestern University, Evanston, Illinois USA. He is the Vice-Provost for Research and the Dean of the Graduate Studies at CSU-Chico, where he is also a Professor of Computer Science. His research interests include computer communications and networks, optical networks, distributed systems, data mining, e-Healthcare infrastructure/architecture/ cloud solution, bioinformatics, information and knowledge management, and object-oriented methodology. He was the Dean of Research and Graduate Studies at CUNY-CSI. He served as a Program Director, CCF/CNS Divisions, CISE Directorate at US National Science Foundation. He is the founder of two conferences: ACM CIKM (Conf. on Information and Knowledge Management) and IEEE IC3N (International Conf. on Computer Communications and Networks).