International Journal of Computer Applications Technology and Research
Volume 1– Issue 3, 64-69, 2012

Healthcare Web Services by E-Governance

Rajan Datt
Institute of Technology,
Nirma University,
Ahmedabad, India

Priyanka Tripathi
Institute of Technology,
Nirma University,
Ahmedabad, India

Abstract: As India is one of the fastest developing countries in the world, it is important to improve the quality of our health maintenance management and preventive medical care to extend healthy life expectancy. Today's scenario for health care in Indian e governance is in the limit of contacting 75 hospitals of the ISRO Telemedicine network only. Whilst this is currently working best of it, the limitation of this can be retarded by introducing the health care web services to each individual of the country. We believe advanced implementation of Information and Communications Technologies (ICT) may improve the medical services and health maintenance management. As medical science is fast developing and information resource is pouring in, there is urgent need for dissemination knowledge by interlinking primary, secondary and tertiary level health centers by ICT applications. This will help health personal to deliver high quality services. Moreover, IT systems have been built to support different work flows in the health sector, but the systems are rarely connected and have become islands of data. From 2006 onwards corporate IT giants are experimenting for ICT application in health sector both in Government and private hospitals. In this paper, we discuss the potentialities and expansibility of the XML Web Services based on the Adaptive Collaboration (AC) which can be aggregated by the Indian e governance system as a health care web services. We would like to present ways of improving health maintenance service and regional medical services. In order to realize better health maintenance and prevention of disease, we would like to prove that incorporating medicine, life, and work through the XML Web Services is highly effective.

The developed system is using data agent concept in transferring the format of information from different medical database systems to be an international standard format of metadata known as HL7 v3.0 using XML based cloud services called the Medical Cloud system which can take advantage of the Indian cloud revolution.

Keywords: Directory Services, Interoperability, HL7, Healthcare services, E Governance

1. INTRODUCTION

Most of the health information systems today are proprietary and often only serve one specific department within a healthcare institute resulting in difficult interoperability problems. To complicate the matters worse, a patient's health information may be spread out over a number of different institutes which do not interoperate. This makes it very difficult for clinicians to capture a complete clinical history of a patient. [1]

The benefits of utilizing the XML Web Services are the following: [15]

1. It is platform independent therefore it is usable regardless of the type of hardware and software,
2. the connection is highly flexible, collaborative, and compatible with other systems,
3. It avoids overlapping investments of the ICT utilization and development
4. It enables the sharing of the ICT sources, and
5. It offers more flexibility in data process and exchange.

Introducing Web services to the healthcare domain brings many advantages:

1. It becomes possible to provide the interoperability of medical information systems through standardizing the access to data through WSDL [2] and SOAP [3] rather than standardizing documentation of electronic health records.
2. Medical information systems suffer from proliferation of standards to represent the same data. Web services allow for seamless integration of disparate applications representing different and, at times, competing standards.
3. Web services will extend the healthcare enterprises by making their own services available to others.
4. Web services will extend the life of the existing software by exposing previously proprietary functions as Web services.

However it has been generally agreed that Web services offer limited use unless their semantics are properly described and exploited [4-7].

Evidence based clinical practice needs sufficient knowledge [9] on latest development in medical science. Automated information management tools like internet, web based libraries, CME, Electronic Medical Record (EMR), Electronic Health records (EHR), and computerized prescriptions are important components. [10]

1.1 E-Governance

E-Governance is the application of Information and Communication Technology (ICT) for delivering government services, exchange of information communication transactions, integration various stand-one systems and services between Government-to-Citizens (G2C), Government-to Business(G2B),Government-to-Government(G2G) as well as back office processes and interactions within the entire government frame work.[1] Through the e-Governance, the government services will be made available to the citizens in a convenient, efficient and transparent manner. The three main target groups that can be distinguished in governance concepts are Government, citizens and businesses/interest groups. In E-governance there are no distinct boundaries. [13]

1.2 Privacy vs. Safety

Health care records often contain sensitive data, which could potentially harm a person's reputation or private life, should it

be exposed to unauthorized people. More seriously, though, these records are the basis on which a patient receives care, and errors caused by negligence, malicious intent, or the like can potentially cause physical harm. [8]

For these reasons, health care records are surrounded by security measures. Ensuring the confidentiality of information while in transit from one practitioner to the next, and while being stored, is imperative to avoid eavesdropping by unauthorized individuals.

Thus organizations that handle sensitive data and the authorized personal who are given the right to access those data should be bounded by law [11 - 12] to ensure that only authorized staff gains access. [8] Moreover the system should have proper, faster and simpler authentication measure.

2. ARCHITECTURE

2.1 Security architecture

Various components of this architecture are

1. A trusted system Security Token Service(SSTS) having a predefined maximum limit of validity
2. Web Services Client (WSC) which are the client computers from where the authenticated personals can refer the system
3. Web Services Providers(WSP) are the provider systems which provides the web services in demand
4. SAML tokens

Security Assertion Markup Language (SAML) is an XML-based open standard for exchanging authentication and authorization data between security domains, that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions). SAML is a product of the OASIS Security Services Technical Committee. [14]

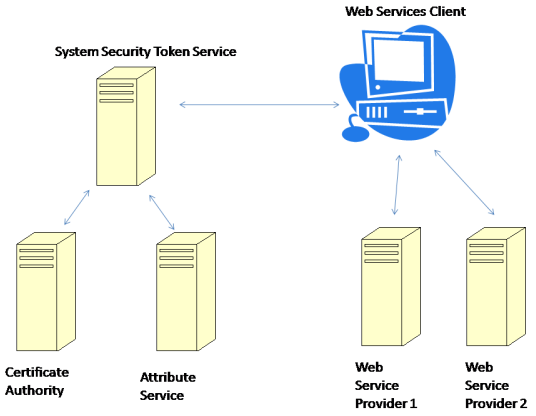

Figure 1 Security and Authentication Architecture

Following steps can be followed for authentication process of the authorized personnel on the system providing the private and secure data about the patients and other details.

1. The user to the system by logging in from a general Web Service Client (WSC). This Client then builds an SAML with attributes and credentials of that user.
2. The System Token Services(SSTS) checks that
   a. the credential of the WSC system is valid
   b. the Web Service Provider(WSP) system certificate is valid and not revoked
   c. the user's credential is valid
   d. the user's certificate is valid and not revoked
3. The SSTS now seeks to verify that the client-specified core attributes are valid by using backend attribute services. Some of these verified attributes are cached for a short period for optimization purposes.
4. If everything is OK, the security token is digitally signed by the SSTS and returned to the WSC.
5. The security token can now be used in interactions with different WSPs until it expires.
6. Upon receipt, the WSPs validate the security token by verifying the SSTS credentials and leverage the embedded attributes for logging and authorization.
7. Finally a result, i.e. business information or an error is returned.

2.2 Service Oriented architecture for healthcare

There are standards that expose the business logic in the healthcare domain such as HL7 [16], which use the messaging technique.

Electronic Healthcare Record (EHR) based standards such as CEN TC251 [17], ISO TC215 [18] and GEHR [19], on the other hand, define and classify clinical concepts that make up the patient records. Such standards offer significant value in developing ontologies to express the semantics of Web services.

But HL7 events are usually very complex containing innumerous segments of different types and options. Moreover the party invoking the Web service must be HL7 compliant. All or some of this data may be coming from different systems that do not interoperate. This in turn, creates the need to retrieve these partial results probably through finer granularity Web services.

In order to define the granularity of Web services, we can refer to Electronic Healthcare Record (EHR) based standards from major standard bodies like CEN and GEHR. These standards define metadata about EHR through "meaningful components". [1]

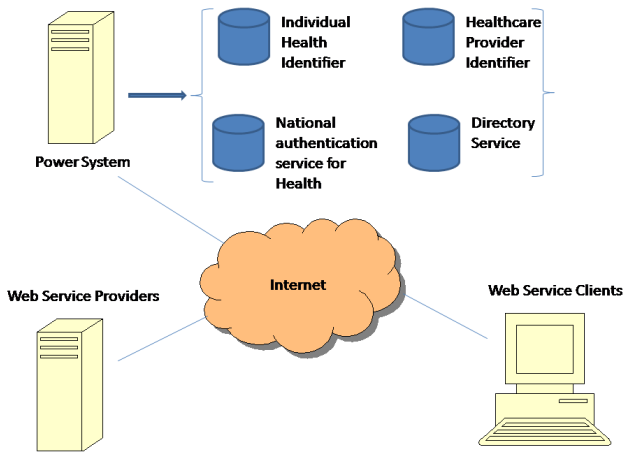

Figure 2 Service Oriented Architecture (SOA)

Generally, health information is stored over a number of different WSP. A national Power system must be available for the provision of directory services to determine the distributed locations of the source systems holding the related health records. Our proposal [20] addresses this need by defining a model to support secure communications between healthcare providers and the Power System in the national e-health environment as shown in Figure 2.

Proposed architecture defines the required constructs to share and transfer healthcare information securely between healthcare providers and the authorized national Power System. This architecture proposes that the
Power System should be built on a high trust computer platform.

Since the Power System is itself a critical application under any operating system, so Power System must be protected from even internal threats through the use of modern "flexible mandatory access control (FMAC)" structures. Under such an operating system, and as distinct from the less secure "discretionary access control (DAC)" systems, even a systems manager may not have permission to access the health record data. In simple terms, in these systems there is no "super-user" capable of obtaining access to all system resources at any time. If an individual name server system is "captured", propagation of exposure will not extend beyond the compromised application itself, a vital concern in any e-health record indexing structure. Such systems exist and are commercially available, e.g. the "Secure LINUX (SELinux)" [21] systems, "Solaris/SE" [22] system, etc.

2.2.1 Power System

The load of the national Power System should be relatively lightweight to perform e-health indexing services efficiently. This can mitigate the Power System explosion and traffic bottleneck risks. Such an approach is favorable in a geographically large country such as India. To maximize the efficiency of the indexing services, the proposed Power System does provide network connectivity services, messaging translation, addressing and routing functions and extensive logging of all message access. These services can be performed at the level of the WSP, which is detailed in Section 2.2. The access control and authorization process is best performed close to where the source system is, as each healthcare service provider might implement the service differently based on its own WSP access requirements. There are no centralized network provisions to handle peer-to-peer communications; each service must manage its own interface to the network.

The Power System will be a centralized facility run at a national level. It is envisioned that the directory service is devised in the context of a DNS, which uses hierarchical distributed database architecture. Our proposed national Power System performs common and fundamental functionalities including:

- Identification and authentication, and
- Directory services.

2.2.1.1 Identification and authentication

Identification and authentication services is same as the security architecture given in Section 2.1

2.2.1.2 Directory services

The Directory Service is one of the fundamental services in national e-health infrastructure. Since healthcare data are located at various places, directory services are used to identify and locate the available information. The Directory Service in the Power System provides a mechanism for obtaining the necessary information for invoking a service. This information contains the network location of the service, the digital certificate required to use it and other information required to invoke the service. It is envisaged this will be specified in Web Services Description Language [23] (WSDL) format, which equates to Service Instance Locator (SIL)

2.2.1.3 Operation of the Directory Services

The service patterns can be divided into two broad categories: synchronous and asynchronous services. A synchronous service occurs in direct response to a request. An asynchronous service has no relationship between the events. For example, to request a specific individual's health records is a synchronous service. To send out a discharge summary report to a healthcare provider is an asynchronous service.

With a synchronous service, when interacting with the directory service the requesting entity will provide proof of their identity and the IHI associated with the records they are requesting. Once the requester has been authenticated by the Power Server, it will respond with the following:

1. A signed token attesting to the identity of the requester ({token}SignIS_PrivKey) and
2. A list of service instances containing health records for the person identified by the IHI (Service_Instance_1,...,Service_Instance_N).

The entire response is signed so that the requester can be assured that it is a legitimate response from an authorized Power System and that any alterations to the response will be detectable. The confidentiality of both the requester and the individual identified by the IHI is maintained.

The token is signed independently of the entire response in order that it can be reused with requests to each service instance. The full response is depicted in Figure 3.

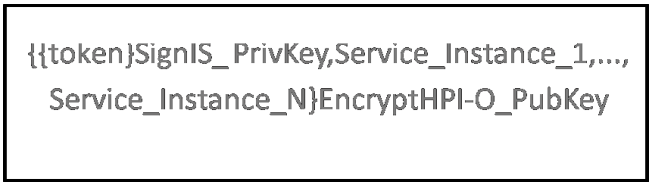

Figure 3 Service Instance Response Message Format

The service instance information contained in the response identifies the target system location and information necessary for securely invoking that service.

This may include, but will not be limited to the credentials certificates required to access the service. The signed token provided in the Power System response may be the only credential required, in which case the effort expended by the Power System in authenticating the requester is reused. It is, however, conceivable that additional authentication may be required by a given service instance. For example, the requester may need to prove that they are a member of a given practice or college of medical practitioners.

With an asynchronous service, such as when a discharge summary message needs to be sent to the patient's primary healthcare provider, the healthcare provider issuing the summary queries the Power System for WSP, location and the digital certificate, credentials and then signs and encrypts the discharge message prior to transmission.

2.2.2 WSP

2.2.2.1 Peer-Entity Authentication

Many proposals are only concerned with the authenticity of the requesting entity (i.e. one-way authentication) but fail to address the importance of two-way authentication. Proposed architecture provides a mutual peer-entity authentication service complying with the ISO 7489-2. To authenticate the authenticity of the Power System, the service requesting entity must validate the certificate of the Power System. Once the authenticity of the national Power System is assured, the Power System authenticates the identity of the healthcare service requesting entity. In this sense, the authentication service of the Power System acts as a notarization mechanism in line with the philosophy of peer-entity authentication stated in ISO IS7498-2.

2.2.2.2 Provision of Data Protection

As various healthcare organizations may have their own specific access authorization requirements and processes, access authorization is best performed where the resource system is located. Once the requesting entity's identity is authenticated, the request of particular healthcare information is presented to the target service provider.

The HIP of the target service provider will provide the verified identity and the profile of the requester to the authorization logic unit to perform access decision making. The authorization decision depends upon the requesting entity's profile and defined privilege management policy. The implementation of the authorization logic unit is based on the "Sensitivity Label" function.

2.2.2.3 Interoperability Platform

Health Level 7 (HL7) 4 can be used as the national standard for the electronic exchange of health information. WSP provides an interoperability platform by incorporating an HL7 Interface Engine and Message Mapping Sets conforming to the HL7 v3.0 Message Standards for healthcare information exchange. HIP also incorporates an HL7 Interface Engine and Message Mapping Sets for messaging Interoperability.

HL7 Interface Engine

Any non-HL7-compliant data contents are translated into the HL7 standard format (XML-based data structure) by the HL7 Interface Engine prior to information transmission. The HL7 Interface Engine contains a set of mapping algorithms to map data contents with an appropriate HL7 Message Template to generate an HL7 message.

Message Mapping Sets

The Message Mapping Sets contain a repository of HL7 Message Templates for various clinical and administrative messages. Each set provides one HL7 Message Template to serve for one clinical or administrative message. Message Mapping Sets will be designed and developed to meet the current healthcare service needs and will be imported into WSP. The HL7 Message Template guides and directs data contents to form an HL7 message.

HL7 Clinical Document Architecture (CDA)

HL7 Clinical Document Architecture (CDA) provides a framework for clinical document exchange. WSP imports the HL7 message into a CDA document. This CDA document is also associated with an appropriate style sheet. The CDA document and the style sheet will be sent to the requesting entity through Web services. The requesting entity renders the received document with the style sheet in a human-readable form with a Web browser.

2.2.3 Key Information Flows

2.2.3.1 Peer-Entity Authentication Process

Follow the steps given in Section 2.1

2.2.3.2 Health Record Enquiry Process

1. The service request, containing the patient's IHI and requester's HPI-I, is sent to the Directory Services of the Power System to inquire which health providers hold the health records of the specific patient.
2. The Directory Services of the Power System responds with a token and a list of the service instance information for service invocation to the requesting entity. This token indicates the requester identity assertion to enable single sign on for service invocation.
3. The requester verifies the received information and then contacts each target service provider for service invocation. The requester sends the request including the token with other necessary information to invoke the service.

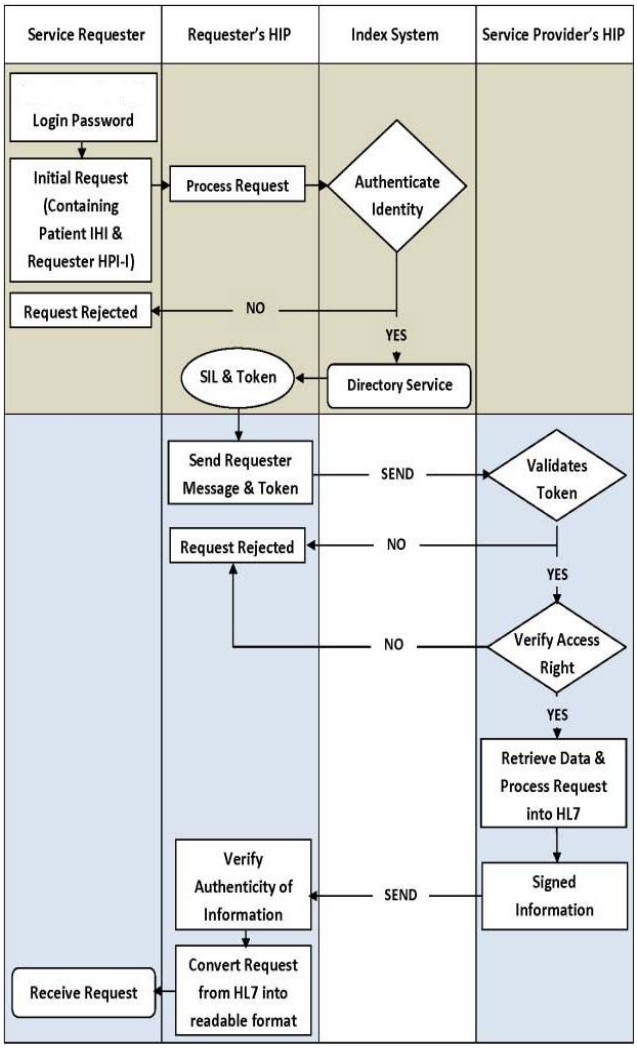

Figure 4 Information Flow

2.2.3.3 Verification and Authorization Evaluation Process

1. Each target service provider validates the request message containing the token and other necessary information for service invocation.
2. In turn, the request is passed to the authorization logic to make an access authorization decision based on the service requester's profile indicated in the ticket and any additional authorization attributes which are mutually agreed by the policy.

2.2.3.4 Provision of Requested Health Record Process

1. If the access is granted, the service provider extracts the health record from the data source.
2. The service provider processes the requested health record into the HL7 message format.
3. The target service provider sends the signed and encrypted information to the requester.
4. The service provider records the information access for auditing purposes.

2.2.3.5 3.5) Reception of Requested Health Record Process

1. The requested information arrives at the service requester's HIP.
2. The service requester's HIP verifies the information arrived and then extracts the requested information which is in HL7 message format.
3. The message must be presented in a human readable format. The representation of HL7 message is rendered and displayed to the requester

3. CONCLUSION

Many people recognize the need of improving the quality and efficiency of health maintenance management. In order to improve the quality of the healthcare management system, sharing information among individuals, patients, hospitals, clinics, medical institutes, and pharmacies is imperative.

XML Web Services enables many people to contact and stay in close touch with physicians and outside mental health professionals at any moment when necessary through network. Therefore, utilization of the XML Web Services would generate innovative ways for the people to maintain and improve their mental and physical health.

In this paper we have presented a healthcare system that uses the Service Oriented Architecture as a basis for designing, implementing, and deploying, managing and invoking healthcare web services. Healthcare requires modern solutions, designed and implemented with modern technologies that encourage healthcare professionals and patients to adopt new procedures that can improve the presentation and delivery of healthcare. Multimedia input and output, particularly graphics and speech, makes the system seem less computer-like and more attractive to users who are not computer-oriented.

This paper proposes following Basic perspectives:

Architecture proposed. A trusted architecture for the Power System which provides the critical solution to determine the locations of distributed health records. This Power System plays a vital role in the national e-health scheme for identification and authentication and directory services. The Power System, therefore, must be a high trust system running on a trusted platform; and

Authentication levels. Users and systems can be authenticated with different degree of certainty, depending on the credentials that the principal presents

Maximum performance. The number of requests/messages is minimized. When trust has been established and the user has logged in to the federation, the WSC and WSP communicate directly with no third party involved.

Presently ICT implementation in health services is in infancy but its further use in both medical education and healthcare industry will revolutionize the healthcare provided by Government hospitals, corporate sector. Finally good quality health care delivery at doorstep in low cost would safeguard national health leading to economic growth.

We believe that our proposal to apply the Web Services would make a substantial contribution to the healthcare and medical field to realize the patient-oriented services.

4. REFERENCES

[1] Dogac, G. Laleci, S. Kirbas, Y. Kabak, S. Sinir, A. Yildiz, Y. Gurcan," Artemis: Deploying Semantically Enriched Web Services in the Healthcare Domain", Software Research and Development Center Middle East Technical University (METU)

[2] Web Service Description Language (WSDL), http://www.w3.org/TR/wsdl

[3] Simple Object Access Protocol (SOAP), http://www.w3.org/TR/SOAP/

[4] S. A. McIlraith, T. C. Son,H. Zeng,"S emantic Web Services", IEEE Intelligent Systems, March/April 2001, pp. 46-53.

[5] S. A. McIlraith,T . C. Son,H. Zeng, "Mobilizing the SemanticWeb with DAMLEnaled Web Services",Semantic Web Workshop 2001, Hongkong, China.

[6] E. Motta, J. Domingue, L. Cabral,M. Gaspari,"I RS II: A Framework and Infrastructure for Semantic Web Services",2n d International Semantic Web Conference,Flor ida, USA, October 2003.

[7] M. Paolucci, T. Kawamura,T . Payne,K . Sycara, "Semantic Matching of Web Services Capabilities", in Proc. of Intl. Semantic Web Conference,S ardinia,Italy , June 2002.

[8] Esben Dalsgaard, Chair, SOSI steering committee Digital Health Denmark (SDSD), Kåre Kjelstrøm Solution Architect Silverbullet A/S Skovsgaardsvaenget, Jan Riis Solution Architect / Project Manager, "A Federation of Web Services for Danish Health Care"

[9] Lele R.D (2008) ," ICT in day-to-day Clinical Practice Postgraduate medicine" API and ICP 2008 Vol. XXII. pp. 3-9.

[10] Subash Chandra Mahapatra (Department of Medicine, MKCG Medical College, Berhampur, Orissa, India) , Rama Krushna Das (National Informatics Centre, Berhampur, Orissa, India) and Manas Ranjan Patra(Department of Computer Science, Berhampur University, Berhampur, Orissa, India), "Current e-Governance Scenario in Healthcare sector of India"

[11] Blobel B, Nerdberg R et al, Modelling privilege Management and access control, "International Journal of Medical Informatics", 2006, 75:597

[12] Han Song, Skinner Geoff et al, "A Framework of Authentication and Authorisation for e-Health Services" . 2006 ACM 1-59593546-0/06/0011 Pages: 105-6

[13] http://en.wikipedia.org/wiki/E-Governance

[14] http://en.wikipedia.org/wiki/Security_Assertion_Markup _Language

[15] Mayumi Hori & Masakazu Ohashi, "Applying XML Web Services into Health Care Management", 0-7695-2268-8/05/$20.00 (C) 2005 IEEE

[16] Health Level 7 (HL7), http://www.hl7.org

[17] CEN TC/251 (European Standardization of Health Informatics) ENV 13606, Electronic Health Record Communication http://www.centc251.org/

[18] ISO TC215, International Organization for Standardization, Health Informatics Technical Committee http://www.iso.ch/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=4720

[19] The Good Electronic Health Record, http://www.gehr.org

[20] Min Hui Lee, Zi Hao Ng, Jin Hong Foo and Weihao Li, Vicky Liu, William Caelli, Jason Smith, Lauren May, "A Secure Architecture for Australia's Index Based E-health Environment"

[21] http://docs.redhat.com/docs/enUS/Red_Hat_Enterprise_Linux/6/pdf/Security-Enhanced_Linux/Red_Hat_Enterprise_Linux-6-Security-Enhanced_Linux-en-US.pdf

[22] http://www.oracle.com/us/products/servers-storage/solaris/solaris11/overview/index.html

[23] WDSL is used for describing how to access the network services in XML format. More detail is available at http://www.w3.org/TR/wsdl#_introduction accessed 30/08/2009.