Federated Service-based Authentication Provisioning for Distributed Diagnostic Imaging Systems

Hassan Sharghi, Weina Ma, Kamran Sartipi
Department of Electrical, Computer and Software Engineering
University of Ontario Institute of Technology
Oshawa, ON, L1H 7K4, Canada
{*Mohammadhassan.Sharghigoorabi, Weina.Ma, Kamran.Sartipi*}@uoit.ca

***Abstract*—Diagnostic Imaging systems record and manage the patients' medical images and relevant reports in digital formats. A modern distributed diagnostic imaging system includes PACS (Picture Archiving and Communication System), image viewers, and a large central repository that provides non-proprietary sharing of medical images among clinicians across geographically distributed hospitals. The lack of adequate interface with common infrastructures has made the proprietary PACS systems as closed environments and prevents seamless integration and interoperation with common infrastructures. In terms of security, there is no federated authentication mechanism for PACS systems and each PACS system controls the user identity locally. We propose a service-based middleware for distributed diagnostic imaging systems by employing different types of agents in order to achieve a federated authentication mechanism for such systems.**

***Keywords*-Authentication; Security; Diagnostic imaging repository; PACS; Multi-agent system.**

I. Introduction

Due to the existence of confidential information in the health record, healthcare providers are considered as attractive targets for cyber attack. Hence, medical data disclosure remains in the second place for the highest reported data breaches [1]. IBM and Ponemon Institute released a research report indicating that in the United States the average cost of the stolen records has significantly increased in recent years [2]. Consequently, maintaining the confidentiality of the patients' clinical information is crucial for the majority of healthcare providers.

A modern distributed diagnostic imaging (DI) system provides a non-proprietary sharing of medical images. A DI includes Picture Archiving and Communication Systems (PACS), image viewer, and a large central Diagnostic Imaging repository (DI-r) whose workflow in the system complies with the IHE (Integrating the Healthcare Enterprise) Cross-Enterprise Document Sharing for Imaging (XDS-I) profiles.

With respect to the security aspects, currently access to the medical images is based on a trust model, where each PACS system uses a local authentication and authorization mechanism to grant users to access the patient images. Such a trust model for a distributed DI system lacks federated capabilities to manage user authentication, authorization and preserving consistent security policy rules. The security issue will be more complicated when a proprietary PACS system is subject to integration with the federated DI systems. Moreover, DICOM is the fundamental standard for communicating digital medical imaging which does not provide adequate mechanism for secure communication across PACS enterprises, and hence maintaining the security of resources using DICOM protocols is a difficult task [3].

In this paper, we propose an innovative infrastructure to provide a seamless integration using single sign-on mechanism to authenticate the local users of PACS systems to globally access to the distributed medical images. The proposed infrastructure complies with the IHE profiles and consists of the following technologies: data acquisition agents, administrative agents, central policy management, central policy repository, central metadata repository for images, as well as a service based authentication model. The authentication will be performed by the collaboration of centralized agents and distributed customizable agents [4]. Overall, this paper presents the following contributions: (i) provisioning an agent based middleware that provides a federated authentication mechanism for every PACS system to globally access to the distributed diagnostic images, and (ii) introducing DICOM proxies that enable the PACS systems to utilize the authentication services provided by the security middleware.

The remaining of this paper is organized as follows: Section II investigates the related work to our approach. In Section III we describe the technologies and standards that are applied in designing the proposed infrastructure. In Section IV we present the proposed federated authentication model. Section V discusses the implementation aspects of the infrastructure, and Section VI provides some concluding remarks.

II. Related Work

Identity management in heterogeneous environments in which participating systems follow different standards is a complicated task. Wolf et al. [5] designed a meta model based on the similarity between SAML and WS-* (WS-Trust and WS-Federation) in order to describe the federated authentication. This model considered the meaning of data based on the context of the message. To test this model, they assumed that a federated identity management was already configured, but practically providing a federated system in a heterogeneous environment is a challenge. The lack of an effective trust management mechanism is a barrier for implementation of the federated identity management based on existing standard such as SAML. Therefore, Jiang et al. [6] designed a new component called Trust Service Provider (TSP) to manage trust relationship between federation parties.

OpenID is a technology for federated identity management that enables users to obtain access to various services using a single set of authentication credentials. It attracts remarkable consideration to authenticate the users in cloud environment so that Khan et al. [7] proposed OpenID-authentication-as-a-service for open source cloud. OpenID is more flexible than SAML because OpenID provides on-demand association as opposed to pre-established association between OpenID providers and service providers. Targali et al. [8] proposed an approach to facilitate secure and seamless mobility across heterogeneous network by applying federated identity mechanism. They combined the OpenID workflow with an efficient mobility management protocol to access networks that users have no prior subscription. Ma and Sartipi [9] applied an agent to authenticate the PACS users by OpenID provider in their proposed infrastructure for secure medical image sharing. We continued their work and in this paper, we propose an agent-based middleware and distributed generic agent for each subsystem to make a federated infrastructure. Then, the middleware agent in collaboration with generic agent provide federated authentication service by using OpenID standard.

III. Background

DI-r: Diagnostic Image repository is a main component of the modern distributed diagnostic systems consisting of a central repository for recording medical images with the capability of providing a non-proprietary image sharing mechanism that is compliant with the XDS-I profile across the healthcare network. DI-r by means of a centralized storage and server infrastructure provides a long-term record of diagnostic results and reports for the lifetime of a patient. Moreover, DI-r provides capability to integrate with local healthcare network by using DICOM, HL7, and XDS-I profile [10].

PACS: A typical Picture Archiving and Communication System consists of: a medical image acquisition system, which collects digital images from different modalities (X-rays, MRI, CT Scanner, etc.); an archiving system, which stores the patient's medical images and the short term or long term reports, and; image consumers, which can access the images through workstations. PACS systems are located in hospitals within a region and widely used as a distributed image sources for DI solutions in healthcare ecosystem to manage medical images by employing a variety of technologies for acquiring, archiving, and transferring.

DICOM: Digital Imaging and Communications in Medicine standard is the backbone of the modern medical imaging systems and handles effectively acquisition, achieving, transferring, and interpretation workflow within an imaging system [3]. DICOM leverages the TCP/IP protocol and adds its own application layer to augment the basic functionality of TCP/IP. DICOM needs a point to point relationship among the communicating systems; therefore a unique DICOM Application Entity Title (AET) must be assigned to each consumer or source, to allow them to identify each other to share data through DICOM. When the number of sources and consumers increases, such associations significantly increases the administrative and network traffic burden. The second DICOM issue is pertinent to the DICOM network IP addresses that must be static. Static IP addresses are barriers for communication with other systems using dynamic IP addresses. In general, DICOM provides proper facilities to satisfy the exchanging use case within an enterprise as opposed to between enterprises [11].

IV. Proposed approach for federated authentication

IHE has developed several profiles to achieve the security requirements within the healthcare network. The lack of federated capabilities to manage authentication and authorization and lack of consistent access control policy rules are considered crucial challenges in distributed diagnostic imaging systems. Without a federated security mechanism, administrative burden increases significantly to ensure that individuals are properly identified in each system and the consistency of access control rules across all systems has been properly managed. Providing a common infrastructure for user identity management can resolve the foregoing drawbacks. Consequently, we propose a service-based middleware as a common infrastructure that employs an agent-based approach to provide different services to make a seamless integration with the legacy PACS and DI-r systems in order to provide the desired level of security services. Our proposed middleware presents generally two layers of services: i) Communication services with transmission capabilities that are responsible for exchanging messages and ii) Common services which provide the required functionalities that are frequently used by the system users. Such common services are responsible for: authentication of PACS users based on their registered identities; making access control decisions; monitoring the user and resource usage; updating system policy and managing metadata. The middleware provides a federated identity management service, which allows users to authenticate themselves with infrastructure

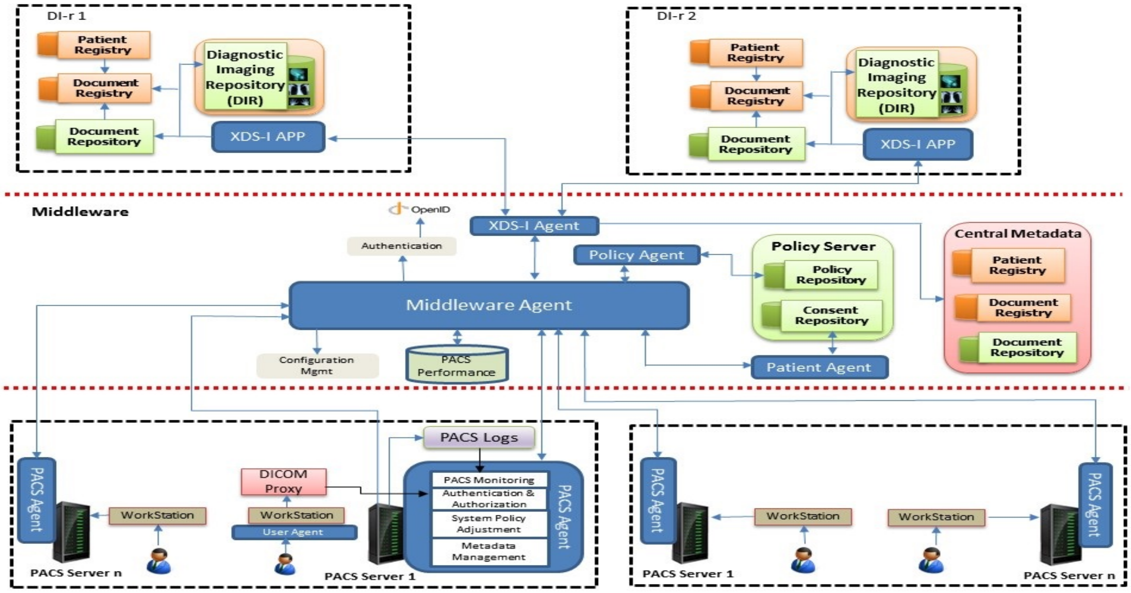

Figure 1. Overall view of the proposed infrastructure to make a secure and seamless connection between the DI-r and PACS systems. Each PACS server is supported by a generic agent called PACS Agent.

that includes a common set of policies for all participating applications in order to share securely and seamlessly the resources. Middleware will use OpenID [12] in order to provide a Single Sign-On (SSO) facility for authenticating the PACS and DI-r users.

Figure 1 shows two types of agents in the proposed multi-agent architecture, namely ”PACS Agent” and ”Middleware Agent” which allow for: extensibility of features, system wide and secure image sharing, federated identity management, and flexible resource attribute query. PACS Agents utilize primitive agents to collect data from users or from databases and are categorized as:

- *User Agent*. This agent enhances the capability of PACS workstation to communicate with web application to prompt the OpenID Identity provider (IdP) links. It allows users to choose one of the IdP links in order to confirm the credential to access the desired resources. In other words, this agent is a wrapper for workstation to provide proper web interface (browser) between real user and IdP.
- *Patient Agent*. The consent directives are defined by patients and are recorded in consent repository. Patient Agent is responsible to add, edit, delete and retrieve records from this repository.
- *Policy Agent*. Federated policies of the whole system are kept in policy repository and managed by Policy Agent.
- *XDS-I Agent*. When image data are transferred from PACS system to central repository in DI-r, XDS-I application extracts the image metadata according to XDS-I profile and saves them in document repository and registry. XDS-I Agent communicates with XDS-I application and keeps a copy of metadata in the central metadata located in the middleware.

Middleware Agent and PACS Agent are considered as Administrative Agents. The Middleware Agent provides various services which can be invoked through appropriate APIs. The main tasks of Middleware Agent are: providing services for authentication; interacting with Policy Agent and XDS-I Agent; sending specific instructions and information to each PACS Agent to customize local policies for making local access control; making access control decision at the middleware level for users who want to access DI-r central repository; recording overall performances of each PACS system; keeping common (federated) policies of the subordinate PACS systems and updating them regularly.

PACS Agent. A customizable generic agent [4] is deployed in each PACS system in order to enhance the PACS system’s functionality to make decision locally and monitor the behavior of the PACS users. PACS Agent along with a User Agent and DICOM proxy provide a mechanism to manage the secure interaction between users and PACS through the middleware. DICOM proxy is deployed between workstation and PACS server to grasp the user request that contains DICOM messages. Then, proxy invokes the authentication service provided by the Middleware Agent via PACS Agent.

DICOM proxy. This application provides capabilities for each PACS system to parse the DICOM message and distribute data across the network. When a user sends a DICOM command through a workstation, the DICOM proxy receives the DICOM message and after recognizing the type of message it invokes the authentication service for current user. If the user is identified as a valid user, this message will be forwarded to the PACS server otherwise the access

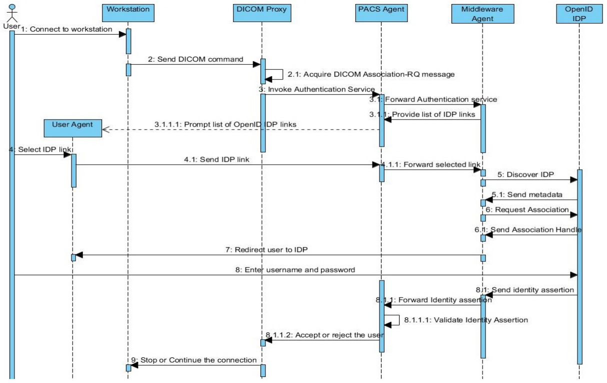
User
Workstation
DICOM Proxy
PACS Agent
Middleware Agent
OpenID IDP
User Agent
1: Connect to workstation
2: Send DICOM command
2.1: Acquire DICOM Association-RQ message
3: Invoke Authentication Service
3.1: Forward Authentication service
3.1.1: Provide list of IDP links
3.1.1.1: Prompt list of OpenID IDP links
4: Select IDP link
4.1: Send IDP link
4.1.1: Forward selected link
5: Discover IDP
5.1: Send metadata
6: Request Association
6.1: Send Association Handle
7: Redirect user to IDP
8: Enter username and password
8.1: Send identity assertion
8.1.1: Forward Identity assertion
8.1.1.1: Validate Identity Assertion
8.1.1.2: Accept or reject the user
9: Stop or Continue the connection

Figure 2. Sequence diagram for authentication of a user, compatible with OpenID protocol.

will be denied.

The proposed Middleware utilizes the OpenID identity management to provide a Single Sign-On (SSO) facility for authentication of the PACS and DI-r users. Such a mechanism relieves the users from memorizing multiple credentials to access services from different providers. Furthermore, in many applications, the service provider is liable to keep safely the user's credentials which increases the service providers' burden. OpenID Provider (IdP), Relying Party (RP) and the user are the main components of the OpenID authentication mechanism. In Figure 1 DICOM proxy requires to verify the user's authentication and hence it plays the role of RP.

V. Implementation

An open source implementation of DICOM protocol has been provided by dcm4che toolkit [13]. Meanwhile, the toolkit can perform the tasks of a PACS system when coupled with a DICOM viewer.

To develop the DICOM proxy, we employed the dcm4che toolkit to manipulate the DICOM protocol. Dcmrcv application works as a SCP (service class provider) and Dcmsnd and Dcmecho applications play the role of a SCU (service class user). We developed a DICOM proxy by reusing two modules dcm4che-core and dcm4che-net to capture DICOM messages and redirect user for authentication. Dcm4che-net module contains some packages that develop and monitor DICOM association to make handshake between two Application Entities (AE). The first action for interaction between two AEs is association which provides a handshake mechanism for AEs to get information about the functionalities of each other and to make an agreement for communication parameters. DICOM uses a structure called Protocol Data Unit (PDU) for association management and message transfer. DICOM proxy based on the value of parameters in A-Associate-RQ redirects the user for authentication by OpenID services. Figure 2 illustrates the message exchange among different entities to authenticate the user.

VI. Conclusion

The proprietary PACS systems adopt different standards and workflows for security provisioning in a distributed diagnostic imaging system. Therefore, it is crucial to provide a federated user identity management for such systems to allow for integration of a large and heterogeneous distributed system. In this paper, we proposed a secure middleware based on a multi-agent system to integrate the distributed PACS systems and different DI-rs. Moreover, a DICOM proxy was developed to extract and parse the DICOM messages in order to invoke authentication services. The authentication will be provided by collaboration of distributed generic agents and a centralized agent via applying OpenID technology. We aim at extending the work by providing an intelligent mechanism for access control by analyzing the behavior of users in order to enhance the policy and security of the whole system.

References

[1] A. Appari and M. Eric Johnson. Information security and privacy in healthcare:current state of research. *International Journal of Internet and Enterprise Management*, 6(4):279–314, 2010.

[2] Ponemon Institute LLC. Cost of data breach study:united states. In *Research Report*, May 2014.

[3] Oleg S. Pianykh. *Digital Imaging and Communications in Medicine (DICOM):A Practical Introduction and Survival Guide, Second Edition*. Springer, 2012.

[4] M. Najafi and K. Sartipi. Modeling service representatives in enterprise systems using generic agents. *Service Oriented Computing and Applications (SOCA)*, 5(4):245–264, 2011.

[5] M. Wolf, I. Thomas, M. Menzel, and C. Meinel. A Message Meta Model for Federated Authentication in Service-oriented Architectures. In *IEEE International Conference on Service-Oriented Computing and Applications(SOCA)*, pages 1–8, 2009.

[6] J. Jiang, H. Duan, T. Lin, F. Qin, and H. Zhang. A federated identity management system with centralized trust and unified single sign-on. In *IEEE 6th International ICST Conference on Communications and Networking in China*, pages 785–789, 2011.

[7] R. H. Khan, J. Ylitalo, and A. S. Ahmed. Openid authentication as a service in openstack. In *In Information Assurance and Security (IAS), 7th International Conference on. IEEE*, pages 372–377, 2011.

[8] Y. Targali, V. Choyi, and Y. Shah. Seamless authentication and mobility across heterogeneous networks using federated identity systems. In *IEEE International Conference on Communications*, pages 1232–1237, 2013.

[9] W.Ma and K.Sartipi. An agent-based infrastructure for secure medical imaging system integration. In *IEEE 27th International Symposium on Computer-Based Medical Systems (CBMS)*, pages 72–77, 2014.

[10] K. Sartipi, K. A. Kuriakose, and W. Ma. An Infrastructure for Secure Shairng of Medical Images between PACS and EHR Systems. In *International Conference on Computer Science and Software Engineering (CASCON)*, pages 245–259, 2013.

[11] D. Mendelson, P. Bak, E. Menschik, and E. Siegel. Image Exchange: IHE and the Evolution of Image Sharing. pages 1817–1833, 2008.

[12] OpenID home page. http://www.openid.net/.

[13] Open Source Clinical Image and Object Management Dcm4che Home Page. http://www.dcm4che.org/.