Cloud-based Identity and Access Control for Diagnostic Imaging Systems

Weina Ma and Kamran Sartipi
Department of Electrical, Computer and Software Engineering
University of Ontario Institute of Technology
Oshawa, ON, L1H 7K4, Canada

Abstract - *The evolution of cloud computing is driving the next generation of diagnostic imaging (DI) systems. Migrating DI systems to cloud platform is cost-effective and improves the quality of DI services. However, a major challenge is managing the identity of various participants (users, devices, applications) and ensuring that all service providers offer equivalent access control in cloud ecosystem. In this paper, we propose an access control infrastructure for secure diagnostic image sharing among Diagnostic Imaging Repositories and heterogeneous PACS (Picture Archiving and Communication Systems) in cloud. We utilize an open standard "OpenID Connect" to provide user-centric Single Sign-On solution, and present the extensions for integrating with patient consent directives and system access control policies. Through combining with the dominant access control model XACML in existing DI systems, the extended OpenID Connect authorization server can provide fine-grained access control.*

Keywords*:* diagnostic imaging; cloud; federated identity; access control; OpenID Connect; XACML.

1 Introduction

With the exploding size of electronic medical records and the fast growth of the diagnostic imaging (DI) market, cloud computing is becoming a preferred solution for image sharing over the Internet using external infrastructure, which allows for accessing to applications and data on demand, any time and from anywhere. Medical data contains sensitive information that may affect the lives of people, so security and patient privacy aspects must be primarily issued. In particular, federated identity management and consistent access control are imperative for cross-domain information sharing and is becoming crucially important with the online healthcare services deployed in cloud environment.

OpenID Connect [1] is an open and decentralized authentication standard that provides a way to verify a user for co-operating sites (known as service providers) without sharing user credential or other sensitive information to service providers. OpenID Connect has broad support from major cloud service providers, enterprise companies, and social networking companies (e.g., Google, Yahoo, Microsoft, and Facebook). According to the OpenID Foundation, the department of health and human services of US Government has joined the OpenID Foundation to create a profile of OpenID Connect and associated projects [1].

OpenID Connect authorization server makes an access control decision based on the resource owner's consent in an interactive way. It is suitable for presenting patient consent directives and their impact on access control. However, as an authorization solution for web services, OpenID Connect does not define a method of enforcing fine-grained system access control polices. In contrast, XACML (eXtensible Access Control Markup Language) [2] is the de-facto attribute based access control standard in DI systems, which provides an extreme fine-grained policy language and processing model. Both system access control polices and patient consent directives enforcement are indispensable parts of the access control model in DI systems. Therefore, combining OpenID Connect authorization flow and XACML model would be a valuable attempt to close the gap.

For the ease of applying a consolidated authentication mechanism, we propose delegating the universal identity management including advanced authentication technology (e.g., biometrics and hardware authentication devices) to the OpenID Connect identity provider. The proposed approach enables users to manage their identities, which minimizes the information disclosure to the service providers. We propose XACML policy based extension of OpenID Connect authorization server to enforce patient consent directives and fine-grained access control rules.

The main contributions of this paper can be summarized as follows: i) designing a user-centric decentralized identity management and authentication service for cloud-based DI systems; ii) proposing fine-grained access control model by combining OpenID Connect authorization server with XACML polices; and iii) enforcing patient consent directives in access control flow.

The remaining of this paper is organized as followings. Related work is discussed in Section 2, and the relevant background technologies are presented in Section 3. In Section 4 our proposed OpenID Connect based federated identity management and access control infrastructure is explained. Section 5 is allocated to a case study, and finally conclusion is presented in Section 6.

2 Related work

Identity federation management enables the users in one domain to securely and seamlessly access data in another domain. Maintaining the user identity repository in each individual domain can lead to information inconsistency and synchronization problems. Meanwhile, the industry trend towards cloud computing and Software as a Service (SaaS) are major drives to shift the federated identity solutions from enterprise-centric to user-centric, and from close-world communication to open standard, where account information is persisted and managed by the third party services. The users are authenticated by co-operating sites (e.g., PACS and DI-r services) using these external services. Relying on external identity services allows users manage their own identity and privacy, and offers the healthcare service providers easier and faster access to the advanced identity management and authentication technology with lower investment.

Due to paradigm shift in federated identity solutions towards user-centric authentication some resent researches focus on providing common authentication mechanism and authorization delegation solutions.

Khan et al. [4] introduced a flexible decentralized authentication service "OpenID-authentication-as-a-service" in the open source cloud OpenStack. Ma and Sartipi [5, 6] introduced an agent-based infrastructure for secure medical image sharing between legacy PACS systems which authenticates users against OpenID protocol. Utilizing OpenID Connect as an identity management and authentication service is not our main target. To provide both fine-grained access control and to support patient consent directives, we need to extend OpenID Connect authorization flows. Ardagna et al. [7] presented extensions to the access control standard XACML and SAML (Security Assertion Markup Language) to enable privacy-preserving and credential-based access control.

OpenID Connect increases the security of integrated systems by putting responsibilities for user authentication to the most expert third party service providers. The organizations that contribute to OpenID Connect are leaders in the developing of advanced authentication technologies such as bi-factor and multi-factor authentication. In addition, the integrated systems still have options to manage their own user information and relationship but outsource the expensive, high-risk tasks of identity verification to external professional service providers. Kakizaki and Tsuji [8] proposed a decentralized user attribute information management method using OpenID Connect for identity verification. By assigning a uniform resource identifier (URI) for all attributes, OpenID Connect identity provider only persists the user's unique ID and related attribute URIs. This feature caters to the healthcare organizations that have concerns about exposing some sensitive patient information to an external identity provider.

OASIS cloud authorization technical committee (CloudAuthZ TC) [9] aims at generating profiles for cloud authorization through making the best of existing, well-designed standards (e.g., XACML, OAuth). The principle idea of CloudAuthZ TC is to reduce the load of authorization engine. Client application obtains a contextual entitlement from authorization engine at the first time of sending access request. After that client application is capable of making decision according to this contextual entitlement without calling authorization engine again, which obviously eases the authorization engine. H. Lockhart [10] explores the possibility of expressing the scope of an OAuth access token by using XACML polices to offer self-contained token, which can be interpreted by the resource server without consulting the authorization server. However, both of these approaches are in their initial stages without practical and successfully applied domains and case studies.

3 Background

In this Section, we introduce the key technologies that constitute the proposed cloud-based identity and access control mechanism for diagnostic imaging.

3.1 Diagnostic Imaging Systems

In medical imaging, PACS (Picture Archiving and Communication System) is a complex integrated system equipped with the necessary hardware and software: digital image acquisition devices namely modalities (e.g., CT scanner, MRI system); digital image storage and archive where the acquired images are stored; and workstations where radiologists view the images [11]. With the increasing demand for collaborative work and sharing of medical information, PACS systems in different hospitals or image centers are interconnected across a distributed environment. Diagnostic imaging repository (DI-r) provides a solution for sharing (publishing, discovery, retrieving and reliably storing) of DI documents across affiliated healthcare organizations. According to the status of DI-r projects across Canada [12], provincial DI-r's have been developed to deliver fast and easy access to diagnostic images to all authorized healthcare providers.

3.2 OpenID Connect

OAuth [3] is an open standard for authorization. It defines specific authorization flows for conveying authorization decisions across network for web applications, desktop applications and mobile applications. OAuth is fundamental to securing service APIs in a simplified way, including: delegated access, avoiding password sharing between users and third parties, and revocation of access. OAuth [3] provides client application an access token for granting access to the protected resource on behalf of the resource owner without sharing credentials such as a password.

OpenID Connect [1] provides an identity n,layer on top of the OAuth protocol. OpenID Connect is a token-based

authentication standard that allows applications to verify the identity of the end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end-user. OpenID Connect provides an identity provider discovery protocol, which dynamically discovers the corresponding identity provider once a user unique ID is given. Apart from identity verification, OpenID Connect allows service providers to use more extensible features such as encryption of identity data, dynamic discovery of identity provider, session management, and to obtain user attributes after authentication. Moreover, OpenID Connect protocol is extended to integrate OAuth authorization process. So OpenID Connect can be used for both authentication and authorization.

3.3 XACML

XACML (eXtensible Access Control Markup Language) [13] defines an access control policy language in XML and a processing model to evaluate access requests based on the defined polices. XACML is an implementation of the attribute based access control, where attributes related to users, resources and environment are inputs into the decision engine. According to the access request and input attributes, the decision engine finds applicable defined policies and makes access decision.

4 Proposed approach

Integrating the Healthcare Enterprise (IHE) has developed a collection of profiles for guiding enterprises in using established standards for an existing IT infrastructure to accomplish interoperability. IHE suggests a trust model where each local diagnostic imaging system is responsible for ensuring that personal health information is adequately protected. A key challenge with this trust model is the lack of federated capabilities:

- User authentication is local to each system that imposes a significant administrative burden to ensure that persons are uniformly identified in each system.
- Access Control rules are local to each system, which means consistency of access rules across all systems has to be managed manually.
- Patient consent directives and their impact on access control are not communicated to each local system electronically and automatically.

After moving to cloud computing, the identity and access control policy synchronization can be extremely complicated with plenty of participants (service providers and service consumers). So deploying a common infrastructure for user identity management, universal access control policy and patient consent directives management is highly needed. The intent is to integrate DI systems with this common infrastructure so that: i) legacy system users can be authenticated against the common infrastructure; and ii) access to patient imaging records can be controlled based on patient's consent directives and system access control polices defined in the common infrastructure.

4.1 Architecture overview

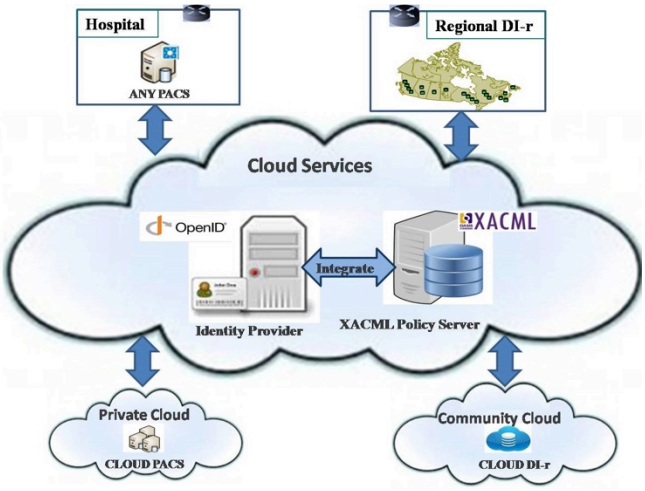


Figure 1. Common identity management and access control method deployed as cloud service.

We propose the design of integrating OpenID Connect identity provider with XACML policy server as cloud service (Figure 1) that: i) provides Single Sign-On user experience to both traditional desktop and mobile users; ii) implements a common service for DI systems to do authentication and authorization; iii) relieves the integrated system administrators from administrative management burden on identity, access control policy, and patient consent directives; and iv) applies ease of utilizing consolidated authentication mechanism to integrated systems, including advanced authentication technology (e.g., biometrics and hardware authentication devices).

Canada Health Infoway stated that the healthcare services deployed in private or community cloud, rather than public cloud, can provide equivalent security level to traditional computing models [14]. So deploying PACS systems and DI-r's to private cloud or community cloud is preferred cloud-based DI solution. We introduce OpenID Connect for creating an identity management and authentication ecosystem for cloud-based DI systems. XACML policy server provides centralized access control policy and patient consent directives management. The existing IT infrastructure in legacy domains is operating based on different technologies, procedures and models. It is not necessary to employ exactly the same access control mechanism across these domains, but it is reasonable that they will agree at the policy level. The integration of OpenID identity provider and XACML policy server will be discussed in next subsection.

4.2 Authentication and authorization flow

OpenID Connect authentication and authorization flow defines six roles as follows: i) "*End User*" is human

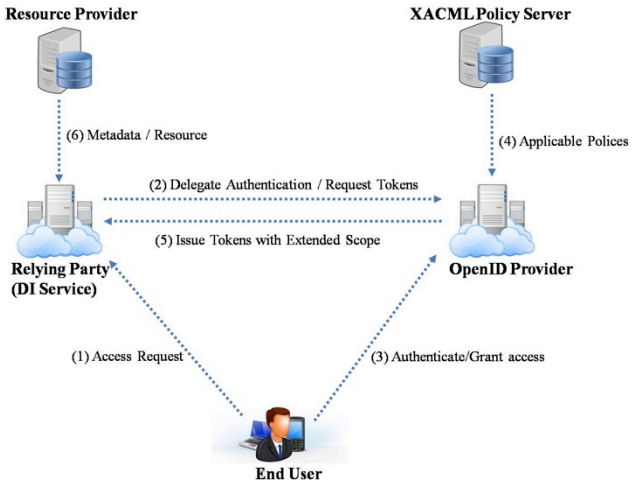


Figure 2. Extended OpenID Connect authentication and authorization flow using XACML Policy Server

participant who wants to access the service (e.g., physician requests to access images from PACS system or DI-r services); ii) "*Resource Owner*" is capable of granting access to a protected resource (e.g., patient may grant a physician or a healthcare organization to access his/her images); iii) "*Relying Party*" is an application (e.g., PACS system and DI-r services) requiring authentication and access grant from OpenID Provider; iv) "*Resource Provider*" manages resources and their metadata; v) "*OpenID Provider*" is an authorization server that is responsible for issuing tokens to Relying Party after successfully authenticating the end user and obtaining granting from Resource Owner; iv) "*XACML Policy Server*" manages access authorization policies and patient consent directives policies.

Suppose that both Resource Owner and End User have already registered to OpenID Provider. In the case that End User and Resource Owner are not the same person, and the Resource Owner is not online to grant or deny the access request, the patient consent directives must be defined and integrated with the OpenID Connect authorization flow.

After successfully authenticated and granted by Resource Owner, Relying Party receives an ID token (which asserts the user identity in a signed and verifiable way), and an access token (credentials used to access protected resource) from OpenID Provider. The access token is typically limited by its "scope" which is issued with access token together. The value of the scope is expressed as a list of space delimited strings, and these strings are defined by the OpenID Provider [1]. For example, a scope of an access control looks like "*profile email address phone*". It means this access token is limited to access Resource Owner's profile, email, address, and phone number. The simple expression of scope is not adequate to describe complicated system access control policies both in syntax and in semantics. So we propose to integrate XACML Policy Server with OpenID Provider, and to represent the scope in the format of XACML policy language. Then the Relying Party may evaluate the scope of access token based on existing XACML infrastructure to make access decisions.

Integration of the OpenID Provider with XACML Policy Server, and the extended authentication and authorization flow is shown in Figure 2.

- OpenID Connect works with any standard Internet browser without any client-software requirement so that the end users, physicians and patients, can set up their devices and applications independently to access DI services from anywhere. Assume that End User has already owned an account with any OpenID Provider. Then he/she initiates an access request and provides his/her OpenID identifier to the diagnostic imaging service (Relying Party). An OpenID identifier for a specific user may look like "myname@example.com" or "http://example.com/myname".
- Relying Party can dynamically discover the location of corresponding OpenID Provider according to the URL "http://example.com". Then Relying Party delegates the OpenID Provider to authenticate End User, and asks for tokens if the access is granted.
- OpenID Provider redirects the End User's browser to a login page to perform authentication. Any authentication method can be used (e.g., password, credentials, information card, and biometrics). After authentication, OpenID Provider checks if End User is also Resource Owner. If they are the same person, OpenID Provider redirects the End User's browser to a granting page and lists the information that will be exposed to Relying Party. The End User can decide to grant or deny this access request. If they are not the same person, OpenID Provider will evaluate this access request against the defined patient (Resource Owner) consent directives.
- XACML Policy Server provides a list of access control polices to OpenID Provider that are applicable to this access request. Such polices can be represented as the scope of access token. As the Relying Party cannot recognize the user related attributes (e.g., user name, role, organization) without consulting OpenID Provider, OpenID Provider should remove or substitute the user related attributes with constant values. Suppose an episode of access control policy is "non-primary physician is allowed to read patient's images from 9:00am to 5:00pm"; if the access session is initialized by a non-primary physician of patient Tom, then the scope of access token is represented as "allowed to read Tom's image from 9:00am to 5:00pm". The method of eliminating variant user attributes from scope reduces the interactions between Relying Party and OpenID Provider.
- The scope of access token specifies what access privileges can be granted to the access token holder. Since the scope does not constitute variant user related attributes, the local decision engine deployed at Relying Party can make access decision by parsing the scope without consulting OpenID Provider.
- Besides of the scope of access token, resource metadata are required to make access control decision. If the access request is granted, Resource Provider returns the demanded resource.

5 Case study

In this section, we describe an end-to-end case study which examines our proposed federated identity and access control architecture. A user account is predefined in OpenID Provider including the following personal information: OpenID identifier "weina@example.com", username "weina" and password, and user attributes such as role (Physician) and organization (Hospital-A). Two access control policies are defined in XACML Policy Server: i) Tom authorizes Hospital-A to access his medical images from Jan 01, 2015 to Dec 31, 2015 (a patient consent directives policy); and ii) physician is allowed to view patient's medical image (a role based access control policy).

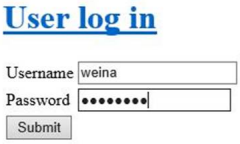
End User named Weina wants to search and view patient Tom's medical images that are created on January 2015. She enters a RESTful request as "GET http://localhost:8080/myregistry/patient/'Tom'/ image/search? 'creationTime'>date'2015-01-01 00:00:00' &'creationTime' < date '2015-02-01 00:00:00'".

The DI-r service receives the access request and delegate OpenID Provider to authenticate the End User. Figure 3-(a) shows redirected page asking for user to enter OpenID identifier. An email address is entered which includes the unique account name "weina" and OpenID Provider host "example.com". Relying party (DI-r service) is able to find the location of OpenID Provider using "example.com". OpenID Provider redirects End User to user login page and needs user input username and password as shown in Figure 3-(b). As End User is not Resource Owner, OpenID Provider queries XACML Policy Server for applicable polices to this access request. Two polices defined above are selected and returned to OpenID Provider. OpenID Provider evaluates the applicable polices according to user related attributes. The End User is a physician and working at Hospital-A, so she is allowed to access patient's medical image from Jan 01, 2015 to Dec 31, 2015. OpenID Provider converts the applicable polices to scope, which constraints the privilege of the issued access token. Figure 3-(c) shows the issued access token, and its scope expressed in JSON (JavaScript Object Notation) rather than a string list. Relying party makes access decision based on the resource and environment related attributes against the scope of access token. As the current date is Feb 2015 and the queried image belongs to patient Tom, the access request is granted. Finally the image is retrieved and displayed in browser as shown in Figure 3-(d).

6 Conclusion

This paper contributes to the domain of diagnostic imaging in cloud computing by providing a solution for federated identity management and access control. We proposed an infrastructure that replaces the existing trust model, which relieves the legacy systems from administrative burdens for identity management and access control policy synchronization. We introduced OpenID Connect as a cloud service to provide user-centric Single Sign-On solution. It allows the user to use one OpenID identifier to sign in to multiple healthcare services, without exposing password or some sensitive information to all these services. OpenID Connect is open to use any modern authentication technology such as smart card and biometrics, which offers the healthcare service providers easier and faster access to the advanced identity management with lower investment. Universal access control policies and patient consent directives are defined in an XACML policy server that is integrated with OpenID Provider.

(a)



(b)

access_token="MXDhGGpKqxZusTu1+Sp9QbSRWaDG/L0IaSWReecSeZHRExbm/+E3nTwfJuYbuYwq6oAEfltW/cAAtgntbKAGn/oH6AQcWU3aIVyrq+GiUSg="
scope=
{
"access": "allow",
"operation": "view",
"resource": "image",
"owner": "Tom",
"time":
{
"from": "Jan 01, 2015",
"to": "Dec 31, 2015"
}
}

(c)

(d)

Figure 3. (a) End User is asked to input an OpenID identifier; (b) User login page for authentication; (c) OpenID Provider issued acces token with extended scope; (d) The pateint's image is displayed in browser.

The applicable access control policies are embedded into the scope that constrains the privilege of the issued access token. The scope can be evaluated by existing XACML decision engine in diagnostic imaging systems without introducing new IT infrastructure change. This research attempts to provide a design for common identity and access control services in cloud-based DI ecosystem and

the implemented prototype proves the feasibility of the design.

7 References

[1] OpenID Connect websit, http://openid.net/

[2] eXtensible Access Control Markup Language (XACML) Version 3.0 (2013), http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

[3] OAuth Community websit, http://oauth.net/

[4] R. H. Khan, J. Ylitalo, and A. S. Ahmed, "OpenID authentication as a service in OpenStack," In Information Assurance and Security (IAS), 7th International Conference on. IEEE, 2011, pp. 372-377.

[5] W. Ma, and K. Sartipi, "An Agent-Based Infrastructure for Secure Medical Imaging System Integration," Computer-Based Medical Systems (CBMS), IEEE 27th International Symposium on. IEEE, 2014, pp. 72-77

[6] K. Sartipi, K. Kuriakose, and W. Ma, "An Infrastructure for Secure Sharing of Medical Images between PACS and EHR Systems," International Conference on Computer Science and Software Engineering (CASCON), 2013, pp. 245-259

[7] C. A. Ardagna, et al. "Enabling privacy-preserving credential-based access control with XACML and SAML." Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on. IEEE, 2010, pp. 1090-1095.

[8] Y. Kakizaki, and H. Tsuji, "A Decentralized Attribute Management Method and its Implementation," Journal of Information Processing and Management 3.1. 2012, pp. 61-69

[9] OASIS Cloud Authorization (CloudAuthZ) Technical Committee, https://www.oasis-open.org/committees/cloudauthz/charter.php

[10] Using XACML Policies as OAuth Scope (2013), https://www.oasis-open.org/

[11] B. F. Branstetter, "Practical imaging informatics: foundations and applications for PACS professionals", Springer, 2009, pp. 33-47.

[12] A. Gauvin, "Status of Diagnostic Imaging Repository (DI-r) projects across Canada", 2010, http://www.camrt.ca/

[13] eXtensible Access Control Markup Language (XACML) Version 3.0, http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html, 2013

[14] Canada Health Infoway, "Cloud Computing in Health White Paper", 2012, https://www.infoway-inforoute.ca/