Security and Cloud Computing: InterCloud Identity Management Infrastructure

Antonio Celesti, Francesco Tusa, Massimo Villari and Antonio Puliafito
Dept. of Mathematics, Faculty of Engineering, University of Messina
Contrada di Dio, S. Agata, 98166 Messina, Italy.
e-mail: {acelesti,ftusa,mvillari,apuliafito}@unime.it

***Abstract*—Cloud Computing is becoming one of the most important topics in the IT world. Several challenges are being raised from the adoption of this computational paradigm including security, privacy, and federation. This paper aims to introduce new concepts in cloud computing and security, focusing on *heterogeneous* and *federated* scenarios. We present a reference architecture able to address the Identity Management (IdM) problem in the InterCloud context and show how it can be successfully applied to manage the authentication needed among clouds for the federation establishment.**

***Keywords*-Cloud Computing; InterCloud; Federation; Identity Management; Security; SAML;**

I. Introduction and Background

Cloud Computing is defined as a large-scale distributed computing paradigm [1]. Commonly, cloud providers are private holding their own virtualization infrastructure, where several virtual machines are hosted to provide services to their clients. The *InterCloud* [2] is instead a new perspective of cloud computing where clouds cooperate with other federated ones with the purpose to enlarge their computing and storage capabilities.

Such perspective opens toward new scientific challenges, including federation, security and privacy. Identity Management (IdM) represents the first issue to be solved, in order to perform the authentication among heterogeneous clouds establishing a federation. Such task is not trivial at all, because it is required a high level of interoperability between different security technologies. In fact, each cloud could hold particular authentication and IdM mechanisms which can be different from each other. Moreover, in order to accomplish IdM in cloud computing, an indispensable requirement is to set up a trusted third party responsible both for storing the access credentials and securing them. [3].

With regard interoperability among different computing systems many works are available in literature: in [4] is presented an approach for enabling federation between distributed computing infrastructures, whereas the IdM problem for the cloud users is addressed in [5]. Other recent works focus on the general concepts of IdM and federation: [6] faces the problem of the interoperability between different IdM technologies, instead the IdM problem in a Service Oriented Architecture (SOA) is described in [7]. In [8], it is proposed an agent-based delegation model for secure web services in ubiquitous computing environments based on Security Assertion Markup Language (SAML) [9].

In this paper, we try to face the IdM and authentication issues in a cloud federation scenario, proposing an InterCloud Identity Management Infrastructure (ICIMI).

II. Our IdM Analysis for the Cloud Federation

According to our analysis, we distinguished two types of cloud: *home cloud* and *foreign cloud*. Home cloud is a cloud provider which is unable to instantiate further virtual machines as the capability of its virtualization infrastructure is saturated and, consequently, forwards federation requests to foreign clouds (which leases part of the storage and computing capabilities of its virtualization infrastructure for free or by charge) with the purpose to exploit their virtualization infrastructures.

In a distributed scenario like the InterCloud, composed of hundreds of clouds, the management of credentials could be very hard: each home cloud should manage hundreds of accounts, each needed for the authentication with a certain foreign cloud, which can change over the time. In addition, it is needed to integrate different security technologies.

We summarize such requirements with the concept of “interoperable security”, which comprises: *1) Single-Sign On (SSO) authentication*, a home cloud should be able to authenticate itself once gaining the access to the resources provided by federated foreign clouds belonging to the same trust context without further identity checks; *2) digital identities and third parties*, each home cloud should be able to authenticate itself with foreign clouds using its digital identity guaranteed by a third party. This latter feature is more challenging because it implies a cloud has to be considered as a subject uniquely identified by some credentials.

III. IdM Using The IdP/SP model

The “IdM/SP model” allows to solve the SSO authentication problem using a global approach and integrating many security technologies. It includes the following four logical components: *The end-user* is a person or a software/hardware entity that assumes a particular digital identity and interacts with an on-line application; The *User agent*, in the common case of the human interaction, can be a browser or another software application; *The service provider (SP)*

978-0-7695-4063-4/10 $26.00 © 2010 IEEE
DOI 10.1109/WETICE.2010.49

or Relying party, a system, or administrative domain, that relies on information supplied to it by the Identity Provider; *The identity provider (IdP)* or Asserting Party is the system, or administrative domain, that asserts information about a subject. For instance, the Identity Provider asserts that an *end-user* has been authenticated and has given associated attributes.

Such model is also referred as IdP/SP model. SAML is the reference XML-based standard implementing the IdP/SP model that addresses several security scenarios and supports many security technologies. The power of SAML is that it can establish trust relationship between entities with different security mechanisms. SAML is different from other security systems due to its approach of expressing assertions about a subject that other applications within a network can trust. According to the IdM model, SAML uses the IdP and SP concepts.

IV. ICIMI: InterCloud IdM Infrastructure

Our solution to the Intercloud IdM is ICIMI, a distributed system based on the IdP/SP model and composed of hundreds of IdPs interacting with clouds' authentication module. Considering such infrastructure the home cloud and the foreign cloud represent respectively the subject and the relying party, whereas the IdP acts as the third party asserting to a foreign cloud the trustiness of the home cloud identity.

A. Requirements and Objectives

Commonly, in order to allow enterprises to federate themselves, a set of mutual agreements has to be drawn up by means of an a priori configuration. Such approach is not suitable to the InterCloud environment where clouds perform resource composition in a dynamic fashion, depending on the instantaneous workload of the whole InterCloud.

Since each cloud has its own authentication mechanisms, a standard method which provides cloud SSO authentication within the federation should be employed: the more convenient approach to provide a flexible, scalable and dynamic SSO authentication is based on the IdP/SP model. Whatever the *foreign cloud* is, regardless of the authentication mechanism it provides, the above mentioned model allows a *home cloud* to authenticate itself with other foreign clouds. The main advantages of the IdP/SP model applied to our reference scenario are: I) Support to various authentication technologies used by each cloud; II) Cloud SSO authentication; III) Cloud's IdM in federated environment.

Our solution to such issues is based on ICIMI, which extends the IdP/SP model to cloud computing environments. Figure 1 depicts an ICIMI scenario where we assume that the home cloud acts as subject, whereas foreign clouds act as a relying parties having security mechanisms, probably different from each other.

In order to enable the home cloud A to request resources to the foreign clouds B, C, and D, an authentication task has to be performed. In order to accomplish such task the home cloud A needs to create an account on IdPs X and Z which act as asserting parties. More specifically, the IdP X is also trusted with foreign cloud B and C, whereas IdP Z is trusted with foreign cloud D. According to our idea, the home cloud A performs an authentication task once on IdPs X and Z, establishing a trust context, and gaining the access to all the needed resources, because the IdPs guarantee on behalf of it with the foreign clouds. In addition, if home cloud A wants to establish a federation with foreign clouds E, F and G, it does not perform any further operation because trust contexts are already established with IdPs X and Z.

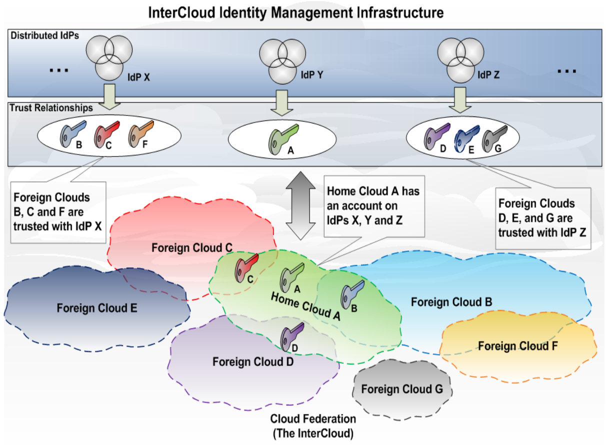
InterCloud Identity Management Infrastructure
Distributed IdPs
...
IdP X
IdP Y
IdP Z
...
Trust Relationships
B
C
F
A
D
E
G
Foreign Clouds B, C and F are trusted with IdP X
Home Cloud A has an account on IdPs X, Y and Z
Foreign Clouds D, E, and G are trusted with IdP Z
Foreign Cloud C
Foreign Cloud E
C
A
Home Cloud A
B
Foreign Cloud B
D
Foreign Cloud D
Foreign Cloud F
Foreign Cloud G
Cloud Federation (The InterCloud)

Figure 1. InterCloud Identity Management Infrastructure scenario.

B. Implementation Practice Using SAML

In our implementation practice we designed a general authentication module placeable inside any cloud middleware responsible to perform the log-in among federated clouds interacting with several distributed IdPs. More specifically, in order to define the message exchange flow between the entities involved within ICIMI, we implement a new SAML profile defining the interaction among the home cloud authentication module(s), the foreign cloud authentication module(s) and the IdP(s).

Considering our reference scenario, if a cloud user performs a resource request which cannot be directly handled by its *home cloud*, or a certain cloud needs external resources to balance its workload, the authentication process defined by our SAML profile starts: the home cloud authentication module will begin the process and, once the *home cloud* identity will be verified, a specific request for external resources is forwarded to the *foreign cloud*.

Considering the scenario depicted in Figure 1, Figure 2 shows the message exchange flow defined by the SAML profile for the authentication of the home cloud A with the foreign clouds B and C. The home cloud A, through its authentication module, begins an authentication process,

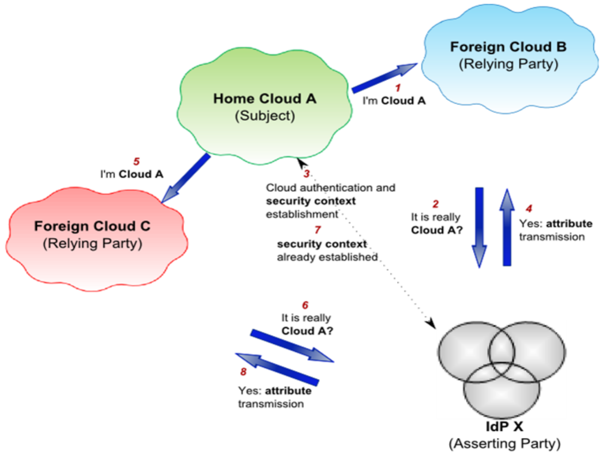

Figure 2. Trust relationship establishment between three clouds.

aimed to temporarily acquire a subset of resources, made available from foreign clouds B (steps 1-4) and C (steps 5-8). Such authentication is performed exploiting the IdP X. In this specific scenario, the authentication module of cloud A acts as the subject (which needs to be authenticated), while the same modules of the foreign clouds B and C act as relying parties which verify the home cloud A's identity before sharing their resources. Otherwise, in another situation, due to a different distribution of workload, noting prevent that cloud B or C could act as home cloud (subject) whereas cloud A could act as foreign cloud (relying party).

In step 1, the authentication module of home cloud A starts the authentication toward the corresponding peer of foreign cloud B, providing its identity. The authentication module of the foreign cloud B forwards the authentication request to the IdP X (step 2). Subsequently, an authentication interaction between the authentication module of the home cloud A and the IdP X is initiated (step 3) and it will lead (if successfully performed) to the generation of a security context for home cloud A. In the last step, the IdP X sends the attributes (i.e. the credential needed for executing local authentication) associated to the authenticated home cloud A back to the authentication module of the foreign cloud B. A similar procedure will also be followed when home cloud A will try to authenticate itself with the foreign cloud C for accessing a subset of resources. Steps 5-6 will be equivalent to the steps 1-2 already described. Differently from the previous authentication process (step 3), since a security context already exists for home cloud A, step 3 will not be performed (step 7): the attributes for authenticating home cloud A with foreign cloud C will be directly sent to the authentication module of the foreign cloud C as shown in step 8.

In the following is shown an example of SAML authentication request sent from the foreign cloud B to the home cloud A used to begin the authentication process with the IdP X.

```
<?xml version=”1.0” encoding=”UTF-8”?>
<S:Envelope xmlns:S=”http://schemas.xmlsoap.org/soap/
     envelope/”>
    <S:Body>
      <ns2:AA-ForeignCloud-B-ResReqResponse xmlns:ns2=”
           http://webservices/”>
         <return>
          <samlp:AuthnRequest xmlns:samlp=”urn:oasis:names
               :tc:SAML:2.0:protocol” xmlns:saml=”urn:
               oasis:names:tc:SAML:2.0:assertion” ID=”dfa6
               ” Version=”2.0” IssueInstant=”2010-01-12T18
               :34:42Z” AssertionConsumerServiceIndex=”0”>
            <saml:Issuer>https://cloudB.net/SAML2</saml:
                 Issuer>
            <samlp:NameIDPolicy
             AllowCreate=”true”
             Format=”urn:oasis:names:tc:SAML:2.0:nameid-
                 format:transient”/>
           </samlp:AuthnRequest>
         </return>
        </ns2:AA-ForeignCloud-A-ResReqResponse>
    </S:Body>
</S:Envelope>
```

V. Conclusions and Future Works

In future, we plan to study the performances of ICIMI, evaluating the amount of authentications and IdP enrollments needed, either employing real testbeds or by means of a simulated environment, including hundreds of clouds dynamically joining and leaving federations.

Acknowledgements

The research leading to the results presented in this paper has received funding from the European Union's seventh framework programme (FP7 2007-2013) Project RESERVOIR under grant agreeement number 215605.

References

[1] I. Foster, Y. Zhao, I. Raicu, and S. Lu, “Cloud computing and grid computing 360-degree compared”, *GCE Workshop*, pp. 1–10, 2008.

[2] Sun Microsystems, Take your business to a Higher Level - Sun cloud computing technology scales your infrastructure to take advantage of new business opportunities, guide, April 2009.

[3] R. L. Grossman, “The case for cloud computing”, *IT Professional*, vol. 11, pp. 23–27, March-April 2009.

[4] C. Vzquez, E. Huedo, R. Montero, and I. M. Llorente, “Dynamic provision of computing resources from grid infrastructures and cloud providers”, *Grid and Pervasive Computing Conference*, pp. 113–119, 2009.

[5] E. Bertino, F. Paci, R. Ferrini, and N. Shang, “Privacy-preserving digital identity management for cloud computing”, *Computer*, vol. 32, pp. 21–27, March 2009.

[6] H. Le and S. Bouzefrane, “Identity management systems and interoperability in a heterogeneous environment” in *International Conference on Advanced Technologies for Communications*, pp. 239–242, October 2008.

[7] K. Traw, S. Yang, and P. Comitz, “Federated identify management in service oriented architectures”, *Integrated Communications, Navigation and Surveillance Conference (ICNS)*, pp. 1–6, May 2008.

[8] H. S. Hwang, H. J. Ko, K. I. Kim, U. M. Kim, and D. S. Park, “Agent-based delegation model for the secure web service in ubiquitous computing environments”, *Proceedings of the International Conference on Hybrid Information Technology*, vol. 1, pp. 51–57, 2006.

[9] SAML V2.0 Technical Overview, OASIS,http://www.oasis-open.org/committees/download.php/11511/sstc-saml-tech-overview-2.0-draft-10.pdf.