D. Nuñez, I. Agudo, P. Drogkaris, and S. Gritzalis, "Identity Management Challenges for Intercloud Applications", *1st International Workshop on Security and Trust for Applications in Virtualised Environments (STAVE 2011)* vol. 187, pp. 198-204, 2011.
http://doi.org/10.1007/978-3-642-22365-5_24
NICS Lab. Publications: https://www.nics.uma.es/publications

Identity Management Challenges for Intercloud Applications

David Núñez[1], Isaac Agudo[1], Prokopios Drogkaris[2] and Stefanos Gritzalis[2]

[1] Department of Computer Science, E.T.S. de Ingeniería Informática,
University of Málaga, E-29071 Málaga, Spain
{dnunez, isaac}@lcc.uma.es

[2] Laboratory of Information and Communication Systems Security,
Department of Information and Communication Systems Engineering,
University of the Aegean Samos, GR-83200, Greece
{pdrogk, sgritz}@aegean.gr

Abstract. Intercloud notion is gaining a lot of attention lately from both enterprise and academia, not only because of its benefits and expected results but also due to the challenges that it introduces regarding interoperability and standardisation. Identity management services are one of the main candidates to be outsourced into the Intercloud, since they are one of the most common services needed by companies and organisations. This paper addresses emerging identity management challenges that arise in intercloud formations, such as naming, identification, interoperability, identity life cycle management and single sign-on.

Keywords: Cloud computing, identity management, intercloud, interoperability.

1 Introduction

The adoption of the cloud computing design pattern is rapidly evolving as more and more organisations reach out for the benefits of distributed datacenters. One of the main advantages of cloud computing is that it provides a model of "*utility computing*"; that is, it is capable of offering on-demand provisioning of computing resources, such as storage, computation and networking. This provision of resources is metered for billing and accounting purposes, making possible a "*pay-as-you-go*" model, which could be beneficial for companies. This paradigm can be put in contrast with previous models, based on the acquisition of equipment and software licences. The main benefits that companies and organisations expect from adopting the cloud computing paradigm are the improved flexibility and scalability of their IT services, as well as the resulting cost savings from the outsourcing of such services [1].

Cloud computing infrastructures combine virtualisation and Service Oriented Architecture (SOA) technologies in order to deliver services through shared computing and storage resources, software, applications, and defined business

processes. Depending of the level of abstraction, these services are referred to as *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS), and *Software as a Service* (SaaS). However, as the resource capability of a single cloud is generally finite, we are moving towards the *Intercloud* perspective, where clouds cooperate with each other in an attempt to evolve their computing and storage capabilities. For such cooperation to be feasible and efficient, this federation of clouds should be established on common semantics regarding addressing, messaging, naming and identification.

Digital identity management services in cloud computing environments are mainly responsible for authenticating users and supporting access control to services based on user attributes. Such services should preserve the users' privacy while supporting interoperability across multiple domains and simplifying management of identity validation. However, as they evolve to Intercloud mouldings, identity management systems should not only be capable of identifying users but also resources that originate from different clouds.

This paper addresses the challenges that arise in the Intercloud mouldings regarding identity management systems that will not only allow for users' and resource's identification but also support and improve interoperability across multiple domains. The rest of the paper is structured as follows: Section 2 provides an overview of the existing identity management approaches in distributed systems while Section 3 addresses the challenges in Intercloud formations. Finally, Section 4 concludes this paper and provides pointers for future work.

2 Identity management in distributed systems

Identity management service provision in traditional IT environments can be performed either through something possessed by user, traits or attributes that constitute a user's real world identity, by something assigned to the user by a third party entity or by something the derives from a user's earlier conduct and attainments. According to [2][3], these functionalities can be classified into the following four categories:

- *Credential identity service*, where the user is identified through pre- assigned credentials such as a digital certificate,
- *Identifier identity service*, where the user is identified through the allocation of specific identifiers, such as an email account or Identification-Card number,
- *Attribute identity service*, where the user is identified through specific attributes that correspond to her real world entity and finally
- *Pattern identity service*, where the user is identified through reputation, honour, trust records and history access records.

As we move on to distributed systems deployment and grid computing, where computing resources and services are shared within virtual organisations, identity management services must provide seamless and secure access to eligible users regardless of the requested resource location [4][5]. Based on their architecture, such identity management systems can be classified into two categories: i) centralised and

ii) federated. In the centralised model, user identification is performed by a central entity, which is responsible for both user identification and authentication. Prior to accessing the requested resource or service, users must first receive authorisation from this entity. This obligatory interaction brings up the disadvantages of this approach regarding administration and privacy weaknesses together with the deficiency of privilege delegation and cross-domain access control. The most renowned systems based on this approach are PKI [6] and Kerberos [7]. The federated model, on the other hand, is based on the establishment of trust relationships between the participating parties. After all participants mutually consent on agreements, standards and technologies they form trust relationships and are then obliged to provide legitimate information about their users whenever another trusted participant requests it. Each relying party can still retain its preferred identification service however once a user is successfully authenticated to a domain, he/she is able to receive personalised services across the federated domains, through the portability of his/her identity. Identity management systems based on this approach include WS-Federation [8], Liberty Alliance Project [9] and Shibboleth [10].

3 Challenges for identity management in the Intercloud

This section addresses the challenges associated with the Intercloud scenario that a complete identity management solution must overcome to leverage the impending advantages of Intercloud applications.

3.1 Naming and identification of Intercloud resources

The nature of the resources involved in the cloud computing paradigm is varied; it ranges from physical components (servers, storage units, etc.) to abstract elements (virtual machines, data repositories, applications, etc.). All these components can be seen as resources of the cloud that are offered to the users. Furthermore, in the Intercloud scenario even clouds themselves could be seen as potential resources to be exploited, as a high-level component capable of offering computation, storage and networking.

Due to this plethora of different kinds of resources, users of cloud computing infrastructures need to be sure of the identity of the resources that they request; that is, they need to know for certain *which* resource is the one they want to request. There is a strong need for appropriate naming and identification mechanisms that enable univocality of resources' identity and permits unambiguous requests. *Naming* is the process of creating a linguistic expression that designates an object [11], while *identification* is the process of distinguishing such an object from the rest in a specific context. Both concepts are closely related, so they are usually grouped together and referred as *identification*. However, we distinguish between the two concepts and treat them separately. These mechanisms are very important, since in most cases they are the basis for advanced functionalities like service discovery, as well as for important security properties, such as authenticity and integrity.

A current approach for the naming and identification of cloud resources is presented in [12], based on the use of XRI [13] and XRDS [14], which are both developed by OASIS. XRI is an extensible scheme for resource naming and identification of resources, while XRDS is an XML-based generic format for resource description and service discovery; XRDS enables the description of resources as well as their associated services, which are called *service endpoints* (SEPs). However, OASIS has recently released XRD 1.0 [15], a new standard for the description and discovery of resources, which supersedes XRDS. The main difference between XRD and XRDS is that, while XRDS describes the services associated to a resource (*endpoints*) in a single document, XRD opts to describe each endpoint in a separate document and to link them all in the resource document. As a consequence, XRDS documents need to be kept up to date with respect with its associated services' attributes, which is something manageable in a private environment where the control of all services is held by the same administrator; however, this is not the case in the Intercloud scenario, so it is essential that each service is described independently, for example, using separate XRD description documents.

3.2 Interoperability of identity information in the Intercloud

As we mentioned before, the outsourcing of internal services is one of the main reasons for the enterprise to adopt the cloud computing paradigm. Some companies are eager to embrace this paradigm because of the cost savings that they expect to achieve as the result of this outsourcing. However, the applications and services within a company are not isolated, and they usually form a network of dependencies, with complex relations among them; some of these services may not be outsourced, so special care must be taken with respect to interoperability, which must be preserved.

Some of the most common services rendered by current IT departments within companies are the ones related with identity management, such as access control, privilege management, authentication and user provisioning. For this reason, identity management solutions for the Intercloud should be interoperable with current identity management systems in the enterprise, in order to enable the outsourcing of such advanced services.

One of the main problems related with the interoperability of identity management systems is the use of different "*languages*" to express the identity information, such as X.509 certificates, SAML assertions or WS-Federation security tokens [10]. That is, there is a *syntactic* obstacle that a complete solution has to deal with. Furthermore, even if the involved parties agree at the syntactic level, the use of different formats, names and meanings for identity attributes also produces incompatibilities. This problem represents a *semantic* obstacle that has to be resolved as well.

The syntactic level problems are tackled through the use of encapsulation and translation mechanisms. In order to achieve real interoperability, it is really important to focus both research and industry effort on the definition and application of standard technologies to facilitate these tasks. For example, WS-Federation includes profiles that enable the use of different formats for expresing the security tokens, like SAML assertions and X.509 certificates; more profiles for other formats can be defined so

that it is extensible. Furthermore, it introduces a special entity called Security Token Service (STS) that is responsible for issuing, managing and validating security tokens; it is also capable of encapsulating and translating between different formats in order to achieve interoperability between different security domains.

Regarding the interoperability issues between different attribute schemes at the semantic level, standards like the X.520 and X.521 ITU-T Recommendations [17][18] and the RFCs 4519 and 4524 [19][20] have tried to solve the problem by identifying common attributes associated to the identity of people and organizations. There exist other initiatives like eduPerson and eduOrg [21], focused in the solving the same problem for educational organizations. However, in the context of the Intercloud, these initiatives are not enough; there is a strong need for solutions that include more types of subjects, resources and services. Another approach to tackle the interoperability problems at the semantic level is the use of ontologies [22][23], which may enable the integration of heteregenous attribute schemes.

As we have seen, the interoperability problems of traditional identity management systems also appear in the Intercloud and they can be classified as syntactic and semantic; both aspects have to be resolved by a complete solution, which should be standard-based.

3.3 Identity life cycle management in the Intercloud

Throughout the life cycle of an entity's digital identity, numerous alternations regarding attributes, authorisation, provision or entitlement can occur depending on an organisation's policy and entity's availability or behaviour. A swift synchronisation of these alternations, to all concerned parties within the Intercloud, seems imperative in order for each entity to have a similar confrontation. Such synchronisation delays could only lead to ineffective resource sharing but also to security vulnerabilities. Depending on the identity management infrastructures deployed within the Intercloud, a common "language" for performing this synchronisation must be adopted. Alternatively, similar to the Certificate Revocation List (CRL) method in PKI, a common repository could be introduced, where every alternation would be announced. In this direction, OASIS has proposed Service Provisioning Markup Language (SPML), an XML framework for managing the provisioning and allocation of identity information and system resources within and between organisations [24].

3.4 Single sign-on for interactions on the Intercloud

The scenario introduced by the Intercloud increases the number of possible interactions that could occur between different actors that participate in the formation. In such interactions, the parties involved are required to mutually exchange identity information, identification and authentication purposes regardless of having previous knowledge of each others identity information or not. From an identity management point of view, the main actors that participate in these interactions are:

- *Intercloud users*, which are the actors that request resources and services, such as human users, external applications (e.g., an IT application from a company), internal applications or cloud providers.
- *Intercloud service providers*, which are cloud providers that are able to offer services or resources to Intercloud users.
- *Intercloud identity providers*, which are cloud providers that are able to authenticate Intercloud users and to share the result of this authentication to Intercloud service providers. They are also responsible for issuing, certifying and managing the identity information of their associated Intercloud users.

In typical cloud environments which support single sign-on functionality, users are able to use the whole spectrum of services and applications without logging-in each time they request a different application or service within the cloud. Similarly, in the Intercloud scenario, users should also be able to access various resources and services offered by different Intercloud service providers, once an Intercloud identity provider has successfully authenticated them. However, as the requested resource could belong to a different cloud, a user's identity information or an equivalent assurance should be transferred to the corresponding Intercloud service provider, without any further actions on the user's part. Consequently, the user's home cloud should be able to perform a single sign-on in order to gain access to the resources offered by another cloud that participates in an Intercloud formation. In this direction, an identity management infrastructure able to support authentication among federated clouds, based on SAML assertions, is proposed in [25].

4 Conclusions

The evolution of cloud computing and the emergence of the Intercloud notion has brought up several challenges regarding interoperability, coherence and standardisation in an attempt to support a dynamic expansion of capabilities. Identity management is an early challenge that must be resolved since identification and authentication must be performed not only for users but for resources as well, within heterogeneous cloud environments. Apart from that, identity management solutions for the Intercloud should be interoperable with current identity management systems in the enterprise, in order to enable the outsourcing of advanced services such as access control, authentication and user provisioning. This paper has addressed emerging identity management challenges regarding interoperability, identity life cycle management and single sign-on that arise in Intercloud formations in an attempt to outline the required characteristics of an efficient identity management system for Intercloud applications. Currently, we are focusing on the interoperability problem, at both syntactic and semantic levels. However, as we have seen throughout this paper, there are several key issues that must be treated and overcome to fully realise the potential of the Intercloud.

Acknowledgements

The work in this paper was partly sponsored by the EC Framework Programme as part of the ICT PASSIVE project (grant agreeement no. 257644) and the ICT NESSoS project (grant agreement number no. 256980).

References

1. Chung, M., Hermans, J.: KPMG's 2010 Cloud Computing Survey (2010)
2. El Maliki, T., Seigneur, J.M.: A Survey of User-centric Identity Management Technologies. In: International Conference on Emerging Security Information, Systems and Technologies, 12-17 (2007)
3. Cao, Y., Yang, L.: A survey of Identity Management technology. In: Information Theory and Information Security, 287-293 (2010)
4. Privacy and Identity Management for Community Services (PICOS), http://www.picos-project.eu/
5. Future of Identity in the Information Society (FIDIS), http://www.fidis.net/
6. Kuhn, R., Hu, V.C., Polk, W., Chang, S.: Introduction to Public Key Technology and the Federal PKI. National Institute of Standards and Technology (2001)
7. Kerberos: The Network Authentication Protocol, http://web.mit.edu/kerberos/
8. WS-Federation, Web Services Federation, http://www.ibm.com/developerworks/library/specification/ws-fed (2007)
9. Liberty Alliance Project, www.projectliberty.org
10. Shibboleth, http://shibboleth.internet2.edu/
11. International Organization of Standardization. Information technologies: Metadata Registries (ISO/IEC 11179-5). http://metadata-standard.org/
12. Celesti, A., Villari, M., Puliafito, A.: A naming system applied to a RESERVOIR cloud. Sixth International Conference on Information Assurance and Security (2010)
13. OASIS: Extensible Resource Identifier (XRI) Syntax V2.0, http://docs.oasis-open.org/xri/xri-syntax/2.0/specs/cs01/xri-syntax-V2.0-cs.html
14. OASIS: Extensible Resource Identifier (XRI) Resolution V2.0, http://docs.oasis-open.org/xri/2.0/specs/xri-resolution-V2.0.html.
15. OASIS: Extensible Resource Descriptor (XRD) V1.0, http://docs.oasis-open.org/xri/xrd/v1.0/xrd-1.0.html
16. Bertino, E., Paci, F., Ferrini, R., Shang, N.: Privacy-preserving Digital Identity Management for Cloud Computing. Data Engineering. Vol. 32 No. 1 (2009)
17. ITU-T Recommendation X.520 (11/2008): The Directory - Selected attribute types (2008)
18. ITU-T Recommendation X.521 (11/2008): The Directory - Selected object classes (2008)
19. Sciberras, A.: RFC 4519 – Lightweight Directory Access Protocol (LDAP): Schema for User Applications. Internet Engineering Task Force (2006)
20. Zeilenga, K.: RFC 4524 – COSINE LDAP/X.500 Schema. Internet Engineering Task Force (2006)
21. Internet2 MACE: eduPerson & eduOrg Object Classes, http://middleware.internet2.edu/eduperson/
22. Wache, H., Voegele, T., Visser, U., Stuckenschmidt, H., Schuster, G., Neumann, H., Hübner, S.: Ontology-based integration of information-a survey of existing approaches. IJCAI-01 workshop: ontologies and information sharing, 108-117 (2001)

23. Priebe, T., Dobmeier, W., Kamprath, N.: Supporting Attribute-based Access Control with Ontologies. In: Proceedings of the First International Conference on Availability, Reliability and Security. IEEE Computer Society, Washington, USA, 465-472 (2006).
24. Service Provisioning Markup Language (SPML), http://xml.coverpages.org/ni2003-06-05-a.html
25. Celesti, A., Tusa, F., Villari, M., Puliafito, A.: Security and Cloud Computing: InterCloud Identity Management Infrastructure. In: 19th IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises, 263-265 (2010)