Anonymous Authentication with a Bi-directional Identity Federation in the Cloud

Fatema Rashid(✉) and Ali Miri

Department of Computer Science, Ryerson University, Toronto, Canada
{fatema.rashid,Ali.Miri}@ryerson.ca

Abstract. Cloud technology offers a completely new set of benefits and savings in terms of computational, storage, bandwidth and transmission costs to its users. In the cloud architecture, user space may be shared across various resources, leading to possible data exposure, and making mapping of users and their privileges a challenging job. Moreover the user has to keep track of many passwords and tokens for different applications. In many setting, anonymity of users accessing some or all services provides in this architecture also need to be guaranteed. In this paper, we propose a bi-directional federated identity management scheme that allows for anonymous authentication of users. Our proposed scheme is applicable to any combination of horizontal and vertical federations, across multiple cloud layers.

Keywords: Federated identity · Anonymous identification · Abstraction layers · Vertical identity federation · Horizontal identity federation

1 Introduction

Cloud computing has indeed revolutionized the concept of computing by promising users unlimited availability and accessibility of resources with convenience. The on-demand concept of cloud computing is at the core of this paradigm. Cloud computing allows users to access or use the services offered by the cloud on the go without actually owning the services through virtualization, web services, encryption, utility computing and the Internet [11]. A key security challenge in such environments is access control and authentication of users by semi-trusted cloud providers. Earlier models of application-centric access control, where each application keeps track of its collection of users and managing those users, are not suitable for a cloud-based architecture [7]. In the cloud architecture, user space may be shared across resources and applications, making mapping of users and their privileges a challenging job. Moreover the user has to keep track of many passwords and tokens for different applications. Federated Identity Management (FIM) deals with the establishment of trust relationships between various security domains by sharing information used for user authentication in order to reduce management complexity and security risks [2]. FIMs involve three main types of entities or players: the user, the Identity Provider (IdP) and the Service

T. Tryfonas (Ed.): HAS 2016, LNCS 9750, pp. 57–64, 2016.
DOI: 10.1007/978-3-319-39381-0_6

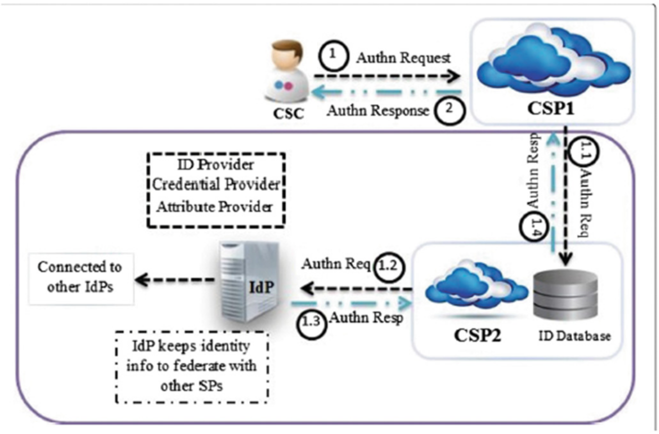

Fig. 1. Federated identity management

Provider (SP). IdPs are responsible for issuing and managing user identities and issuing credentials. SPs are entities that provide services to users according to their identities (see Fig. 1 [5]).

FIM also helps to simplify end-user authentication procedures by employing mechanisms such as single sign on (SSO) [2]. FIM solutions have been used in various applications, such as web resources allocations [7], web services [3], and grid computing [6].

Cloud computing generally operates on three levels of abstraction, namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as Service (SaaS). The IaaS layer includes the use of virtual machines to provide on-demand services to end users. The PaaS layer is a category of cloud computing services that provides a platform that allows users to develop, run, and manage their applications [8]. SaaS layer typically deals with software is licensed on a subscription basis, and is centrally hosted [8]. One should note that there are also sublayer services in the cloud with high utilization and usefulness such as Database as a Service (DaaS) or IDentity as a Servie (IDaaS). Since a typical cloud deployment has a layered structure made of IaaS, PaaS and SaaS, the services provided at these levels should be accessible to users in a secure, but seamless manner. Generally, higher levels of abstraction (layers) in a cloud utilize functionalities provided by lower levels. However, current federated identity solutions are limited to a single level only (e.g. IaaS or SaaS). Therefore if a SaaS provider needs to transfer the credentials of a user to lower layers, he has to implement his own solution, since the lower layers (IaaS and PaaS) are ignorant of any users signed in at the upper level. If the cloud is incorporating multiple IaaS, PaaSs or SaaSs providers interacting with each other, then the problem becomes more complex. FIM solutions over the cloud can hence be broken down into *vertical* and *horizontal identity federations*. Horizontal identity federation is a concept that enables the sharing of resources a Cloud Service Providers (CSP) at a particular service delivery layer such as IaaS, PaaS or SaaS, whereas in vertical identity federation, identities are shared vertically, from SaaS layer to PaaS to IaaS layers or throughout the layers of different cloud architectures [11]. Our proposed identification algorithm in this paper works with any combination of horizontal or vertical identity federations.

Keeping anonymity of users' identities and their activities also poses another challenge. Security has always been listed as of the key hurdles in acceptance of cloud computing as a viable technology, given the loss of physical control users can exercise over their data, applications, platforms or infrastructure resources. Cloud computing therefore requires an entity/user-centric model, where every entity's request for any service is bundled with the entity's identity and entitlement information [1]. The loss of control over users' data implies that in most cases users have to rely on the cloud access rules and policy for protection of their privacy. However, users typically have accept and are subject to different access policies for different CSPs. On-demand architectural set up will also enables CSPs to outsource users resource requirements to third parties, for which users may not have the same trust relationship. Or, for which CSPs will wish to procure requested services to their users through these third parties, while not allowing these parties to learn true user identities.

We therefore propose a merger of anonymous identification requirement with that of federated identity in order to attain the advantages offered by both. The anonymous identification component enables a user to prove his/her identity, without actually disclosing any identity credentials. Our integration of this anonymous identification component with a federated identity is done in such a fashion to make the cloud architecture secure throughout all the layers. Federated identity is integrated from SaaS to IaaS layers. The PaaS layer is used to hide the implementation details from the IaaS layer. SaaS users can access SaaS applications without any interference from the Identity Provider. The integrated identity architecture is based on the concepts presented in [1,10], but is tailored to fit in our scheme of anonymous identification. To the best of our knowledge, our work is the first proposed approach to integrate a bi-directional identity federation with anonymous authentication, which a provide a fine grain access control, while enabling cloud users to utilize cloud services within a federation.

The rest of the paper is organized as follows: Sect. 2 discusses some related work. Section 3 provides the details of the proposed scheme and conclusions are presented in Sect. 4.

2 Related Work

Federated identity with vertical and horizontal dimensions was discussed in [10]. In this work, authors present an approach in which the identities of the users are federated in both horizontal and vertical directions, with the help of a third party IdP. The users can use services from different clouds within the federation at all the three levels, namely IaaS, PaaS and SaaS. In their architecture, they introduced a module called *interceptor*, which could be used for authentication purpose by different users. Another module called *dispatcher* is used to keep a log of users in order to classify them for commercial purposes. This scheme does not take into consideration the need for anonymous identification issue and allows for different configuration setup of the interceptor used for user authentication purposes. In [1], authors introduced the concept of anonymous authentication to prevent misuse of customers' personal information by the cloud. Their anonymous authentication is based on two protocols, which we have explained in the following sections. However, their solution considers the cloud to be single entity, and does not provide any support for the typical layered structure of the cloud and horizontal and vertical federated identity managements.

Our proposed scheme build on these earlier work by combining the anonymous identification and the FIM concepts, which is further expanded to support both vertical and horizontal federated identities.

3 Proposed Scheme

As discussed in the earlier section, our aim is to integrate identity federation with anonymous authentication, in order to enable the users to have a complete control over the decision of with and how much information should be shared among different clouds under one federation. There are a number of benefits to such combination, which produces a comprehensive and secure federated identity environment for cloud users. These benefits include ability to provide Single Sign On (SSO) options. It also supports provisioning of identities within an organization addresses and the provisioning and deprovisioning of several types of user accounts, enabling service providers to reduce the cost of managing user attributes, passwords and login credentials by using trusted identity providers and provision of scalability [2]. Our scheme ensures anonymous authentication which makes it possible to prove a claim or assertion for authentication without disclosing any identifiable data. Within a cloud computing environment, this feature becomes even more useful for ensuring security, when using semi-trusted CSPs for different services. That is, If the users does not want to share their identity information with a specific CSP but would like to use their services, they can authenticate themselves anonymously on these semi-trusted clouds through an Identity Provider (IdP).

The proposed scheme has the advantage of being able to support vertical and horizontal identity federation, as well as anonymous identification. The overall architecture and flow of data of the proposed scheme is represented in Fig. 2.

3.1 Anonymous Identification

To achieve anonymous identification, we use the Fiat and Shamir identification scheme [4]. This scheme has been used in cloud settings for anonymous identification in [1,9], but these schemes did not consider the abstraction levels of the

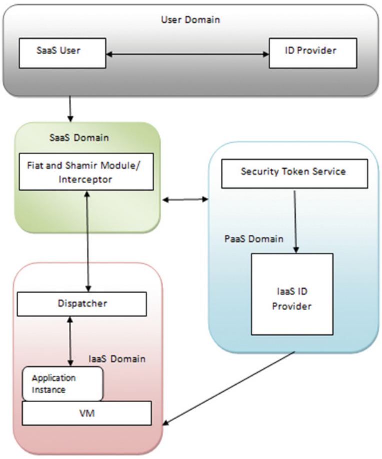

Fig. 2. Architecture of the proposed scheme

cloud. We regard cloud as a layered structure of SaaS, PaaS and IaaS layers, and thus propose to provide vertical and horizontal identity federation. The scheme has two protocols: issuing identity to an entity, and verifying identity of an entity [4]. Firstly the IdP selects a public integer n and a pseudo random function f, where f associates arbitrary strings to elements in the range $[0, n)$. Integer n is the product of two secret prime numbers p and q, where the values of p and q are only known to IdP.

Protocol 1(Issuing Identities by an IdP to a User). IdP formulates a string I, which contains all the relevant information about the user e.g. validity date etc. The IdP then performs the following steps [4]:

- Compute values $v_j = f(I, j)$ for identity information at indices j.
- Pick k distinct values of j for which v_j is a quadratic residue mod n, and compute the smallest square root s_j of v_j^{-1}.
- Issue an identity, which contains I, k s_j values and the selected k indices (For simplicity, one can use the first k indices $j = 1, 2, \cdots, k$).

Protocol 2: Verifying the Identity of the Entity. Fiat and Shamir verification [4] is based on the user A proving the possession of the k s_j values interactively, without revealing their values, or equivalently the bounded identity assigned to the user and his/her general information I by IdP. The main steps of the procedure can be repeated t times, where t can be treated as a security threshold parameter.

- A sends I to CSP, and CSP computes $v_j = f(I, j)$ for $j = 1, \cdots, n$.
- The following steps can be repeated t times to ensure that probability of error is less than 2^{-kt}.

- A picks a random $r_i \in [0, n)$ and sends $x^i = (r_i)^2 \mod n$ to CSP.
- CSP sends a random binary vector $(e_{i1}, \cdots, e_{ik})$ to A.
- A sends to CSP: $y_i = r_i \prod_{e_{ij}=1} s_j \mod n$.
- CSP checks that $x_i = (y_i)^2 \prod_{e_{ij}=1} v_j \mod n$.

CSP will accept the validity of user's identity, if all the t comparison pass the test.

3.2 Federated Identity

The working of the federated identity across the layers of the cloud architecture is explained in this section. It follows the architecture proposed in [10]. In our architecture, a SaaS user accesses the SaaS application interface using a web client, and submits his/her access request to the interceptor, controlling access to the resource. If the interceptor cannot find a valid session for the access request, it asks the user to authenticate himself/herself using credentials provided by an IdP of his/her choice, and accepted by the SaaS provider. The user can use the Fiat and Shamir identification scheme to verify the user identity. The interceptor validates the proof of authentication and requests a new security token from a Security Token Service (STS). The STS and interceptor trust each other for all transactions, which is managed by PaaS. The STS ensures that the user is allowed in the IaaS domain as well. This is where the vertical identity federation is being implemented by allowing the valid users to navigate from SaaS to IaaS with a single valid identity. The STS issues a new token containing the IaaS users' Id and is signed by the STS private key. For the first interaction, the SaaS users get registered accounts on the IaaS identity. A new identification is created for the user based on his SaaS identification. The IaaS identity Provider centralized the account information for all IaaS users, and share this information with the operating systems and thus ensuring that there is no need for account creation on each virtual machine. The interceptor forwards the access request to the application endpoint with the token obtained from STS. SaaS application captures the request and verifies the security token. If it is signed by the STS, it is considered authenticated. The SaaS application uses the IaaS identification embedded in the request to execute the actions on the authenticated user's behalf. There is a trust relationship with the STS, which is maintained by the PaaS administrator. Since the IaaS now recognizes the IaaS user, the operations are performed successfully. The request is then transferred to the SaaS application instance on the specific virtual machine owned by the IaaS user. As we mentioned earlier, that horizontal and vertical federation of identities across the layers of the cloud architecture are the core of our proposed scheme. The IaaS provider stores the minimum and essential account data and user information for the cloud. This information is replicated on different IaaS providers running on different virtual machines [10]. This gives the availability of the application to the user, no matter on which VM, the instance of the application is running. This setup provides the horizontal federation of the identity across all the IaaSs being used, and can provide a single sign on option to users.

4 Conclusion

In this paper, we discussed and focused on some of the security concerns in cloud computing, and in particular issues with user identity and its management. The need of federated identity is highlighted along with its possible benefits, such as support for single sign on capabilities. We discussed the requirement of anonymous identification in the cloud architecture, and proposed a combination of anonymous identification and federated identity solution. We further extend this approach to include both vertical and horizontal federated identity support. Vertical federation of identity aspect of our solution allows a user to choose the identity provider of his/her own choice, where as horizontal federated identity aspects ensures the use of multiple services across a given layer, possibly provided by different CSPs are also supported. Our future plans include the implementation of the proposed concept in the real life cloud settings. We would like to test our anonymous authentication scheme in terms of scalability and security. The implemented scheme should accomodate a large number of users coming from very diverse, but federated clouds.

References

1. Angin, P., Bhargava, B., Ranchal, R., Singh, N., Linderman, M., Othmane, L.B., Lilien, L.: An entity-centric approach for privacy and identity management in cloud computing. In: 2010 29th IEEE Symposium on Reliable Distributed Systems, pp. 177–183. IEEE (2010)
2. Chadwick, D.W.: Federated identity management. In: Aldini, A., Barthe, G., Gorrieri, R. (eds.) Foundations of Security Analysis and Design V. LNCS, vol. 5705, pp. 96–120. Springer, Heidelberg (2009)
3. Nadalin, A.: Oasis: Web services federation language (ws-federation) version 1.2. http://docs.oasis-open.org/wsfed/federation/v1.2/wsfederation.html. Accessed Jan 2016
4. Fiat, A., Shamir, A.: How to prove yourself: practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 186–194. Springer, Heidelberg (1987)
5. Habiba, U., Masood, R., Shibli, M.A., Niazi, M.A.: Cloud identity management security issues & solutions: a taxonomy. Complex Adapt. Syst. Model. **2**(1), 1–37 (2014)
6. Mikkonen, H., Silander, M.: Federated identity management for grids. In: Proceedings of the International conference on Networking and Services (ICNS 2006), p. 69. IEEE (2006)
7. Morgan, R., Cantor, S., Carmody, S., Hoehn, W., Klingenstein, K.: Federated security: the shibboleth approach. Educause Q. **27**(4), 12–17 (2004)
8. National Institute of Standards, Technology: Special Publication 800–146: Cloud Computing Synopsis and Recommendations. National Institute for Standards and Technology, Gaithersburg, May 2012. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf
9. Ranchal, R., Bhargava, B., Othmane, L.B., Lilien, L., Kim, A., Kang, M., Linderman, M.: Protection of identity information in cloud computing without trusted third party. In: Proceedings of the 29th IEEE Symposium on Reliable Distributed Systems, pp. 368–372. IEEE (2010)

10. Stihler, M., Santin, A.O., Marcon Jr., A.L., Fraga, J.D.S.: Integral federated identity management for cloud computing. In: Proceedings of the 5th International Conference on New Technologies, Mobility and Security (NTMS), pp. 1–5. IEEE (2012)
11. Thomas, M.V., Dhole, A., Chandrasekaran, K.: Single sign-on in cloud federation using cloudsim. Int. J. Comput. Netw. Inf. Secur. (IJCNIS) **7**(6), 50 (2015)