Privacy Issue in Federated IDMS for Cloud Computing

Yeongkwun Kim
School of Computer Sciences
Western Illinois University
Macomb IL, USA
Y-Kim2@wiu.edu

Injoo Kim
Department of Computer and Information Science
East-West University
Chicago IL, USA
injoo@eastwest.edu

Charlie Y. Shim
Department of Computer Science and Information Technology
Kutztown University of Pennsylvania
Kutztown PA, USA
shim@kutztown.edu

Abstract— **Federated cloud identity management systems (IDMS) enable users to use the same identity information to access all network services and resources in the trusted domain. Federated cloud IDMS has gained significant attention from the IT industry due to its support of cross organizational boundaries without creating additional user accounts. However, using the same identity information can disclose comprehensive user profile information, such as usage pattern, interests, or the behavior of the user. In this paper, we discuss possible security concerns, especially privacy issues, and ultimately propose a way to preserve privacy in the federated cloud IDMS by use of same single user identity information.**

Keywords - cloudcomputing; federal identity management; privacy.

I. INTRODUCTION

Due to the rapid development of computer and network communication technologies, cloud computing has achieved increased popularity. The National Institute of Standards and Technology [1] defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services." In order to access network services or resources, users are required to present their personal identities for the purposes of authentication. This subsequently results in cloud computing posing potential a significant challenge to the user's information, security realization and privacy protection. Thus, in response, industries have introduced IDMS as a means of managing the identity information of different users [2]. According to deployment architecture, IDMS can be classified into the isolated cloud IDMS, the centralized cloud IDMS, and the federated cloud IDMS [3]. The federated cloud IDMS enables users to use the same identity information to acquire access to all network services and resources within any trusted group of enterprises [4]. For the purpose of authentication, network users typically maintain a set of user identity credentials such as a username/password combination with every service provider. Unfortunately, the number of interactions service provider typically engage in with the user has grown beyond the point of ordinary users' ability to memorize and recall the necessary access information. Thus, using the same identity credential to access network services or resources provided by any service provider has underscored the apparent ease and efficiency of the federated cloud IDMS and a possible solution is Single Sign-On (SSO). However, one of the main problems SSO poses is user privacy. User identity information can be shared with identity provider(s) and service providers, who can obtain the information from the identity provider. Thus, malicious identity and service provider can reveal users' identity information and activities. In this paper, we discuss a possible solution to preserve users' privacy in the federated cloud IDMS based on the SSO.

II. RELATED WORK

The SSO provides the ease of single authentication which subsequently allows users to become automatically logged into all other service providers within the same trust domain, thereby eliminating further manual interaction with the service provider. As such, SSO increases the overall usability of network. SSO system can be classified into pseudo-SSO and true SSO [5]. The pseudo-SSO component manages the service provider specific user authentication information. In the true SSO, the authentication service provider verifies the user. The authentication service provider must establish a trusted relationship with all service providers in order for the SSO to be achieved. Typically, the relationship may be established by a contractual arrangement. The federated cloud IDMS consists of a group of identity providers and service providers. Sharing user information and activities may result in further revealing by malicious providers and users have no control mechanism over disclosure of their identity information. Suriadi and et al. [6] have proposed a mechanism to provide user privacy by allowing users to enact some degree of control of their identity information. In the My Private Cloud project, Chadwick and et al. [7] proposed a trust based approach for federated access to cloud resources.

 ISBN: 978-1-61208-451-0

III. PROPOSED APPROACH

In our proposed approach, we assume that 1) there is a group of trusted third parties that provide identity services to users and service providers; 2) there are two levels of trusted identity providers; 3) identity service providers and actual service providers have a trusted relationship with each other; 4) proper encryption mechanisms are already in place to ensure secure transmission among users, identity providers and service providers. Exchanging security information must be based on the trustworthiness of users, identity providers, and actual service providers. In this paper, as a possible way of preserving users' privacy, we consider a group of identity service providers in a two-level hierarchical architecture. The higher layer (level 2) identity providers act as a central identity server and generate a security token (e.g., random number or nickname) based on the user's registration request. Only these providers know the user's actual identity information. This proposal also includes lower layer (level 1) identity providers for purposes of actual authentication of the authorized users based on the token provided by the user. When the level 2 identity provider receives registration, it generates a token that corresponds to the user's real identity, which in turn ensures the privacy of users. This token is then forwarded to the level 1 identity service provider to cooperate generating a certificate and security key(s) based on the token provided by the user. Thus, the level 1 identity provider does not have any information to identify the user's real identity. And the certificate itself does not reveal the user's real identification. The level 1 identity provider may send the generated certificate back to the level 2 identity provider that retains a record of the user's real identification if needed, while sending the corresponding certificate and security key(s) to the user without storing any relevant information. The level 2 identity providers should not be able to see the security key(s) and certificate. Furthermore, the level 1 identity provider only has information of the token, and the generated certificate and security key(s) based on the token. Government agencies need to be able to access both the level 2 and the level 1identity providers to obtain the user's real identity. Users will not be at risk of having their personal information revealed, even if they log on/off to access network services and resources from any service provider. Figure 1 illustrates the information flow in our proposed approach.

IV. CONCLUDING REMARKS

When we subscribe the new cloud service, it is important for users to firstly complete a registration to accrue a new set of credentials. Unfortunately, users tend to generate weak and easy to remember passwords, which can in turn cause users to easily become targeted by potential security attacks. Thus, one possible solution is to create single sign-on that allows users to authenticate just one time and then be automated for further authentication during the same login session. However, single sign-on caused another security issue, such as user privacy. This is because malicious identity service providers and actual service providers can cooperate to reveal and trace both the real identity and the activities of the user. Hence, in this paper, we proposed a way to mitigate the concerns regarding protecting the privacy of users in the federated cloud IDMS. We believe that the fruits of this work are evident, but remain in need of continued research.

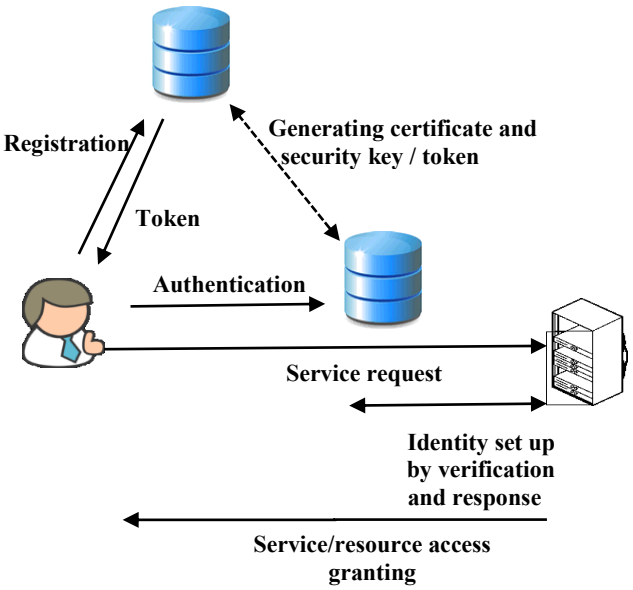

Figure 1. Information flow in privacy preserving SSO

REFERENCES

[1] Vince Lo Faso, "A practical view of NIST's cloud definition", *Global Knowledge*.

[2] M. S. Ferdous and R. Poet, " A comparative analysis of identity management systems", Proceedings of the International conference on high performance computing and simulation (Madrid, Spain, July 2-6, 2012), pp 454-461.

[3] U. Habiba, R. Masood, M. Shibli, M. Niazi, "Cloud identity management security issues and solution: a taxonomy", Complex Adaptive Systems Modeling. Vol. 2, No. 5.

[4] Y. Cao and L. Yang, "A survey of identity management technology", Proceedings of the IEEE International conference on information theory and information security (Beijing, China, December 17-19, 2010), pp 287-293.

[5] A. Pashalidis and C. Mitchell, "A taxonomy of single sign-on systems", Proceedings of the 8th Australasian conference on Information security and privacy (Berlin, Heidelberg: Springer, 2003), pp 249-264.

[6] S. Suriadi, E. Foo, and A. Josang, "A user-centric federated single sign-on system", Proceedings on IFIP International conference on network and parallel computing workshops (Liaoning , China, September 18-21), pp 99-106.

[7] D. Chadwick, M. Casenove, and K. Siu., "Security APIs for My Private Cloud – Granting access to anyone, from anywhere at any time", Proceedings of the IEEE conference on cloud computing technology and science (Athens, Greece, 2011), pp 792-798

 ISBN: 978-1-61208-451-0