2015 2nd International Conference on Information Science and Control Engineering

Managing Identities in Cloud Computing Environments

Xiaoqi Ma
School of Science and Technology
Nottingham Trent University
Nottingham, UK
xiaoqi.ma@ntu.ac.uk

***Abstract*—As cloud computing becomes a hot spot of research, the security issues of clouds raise concerns and attention from academic research community. A key area of cloud security is managing users' identities, which is fundamental and important to other aspects of cloud computing. A number of identity management frameworks and systems are introduced and analysed. Issues remaining in them are discussed and potential solutions and countermeasures are proposed.**

Keywords—Cloud computing, security, identity management

I. INTRODUCTION

Cloud computing is now becoming a more and more popular concept appearing in all kinds of articles that discuss future trend of computing models. A *cloud* can be regarded as a large-scale federation of various computing resources, including computation, storage and network bandwidth facilities. Cloud computing service providers provide their services in a number of fundamental models [1]. The most widely used models are *infrastructure as a service* (*IaaS*), *platform as a service* (*PaaS*), and *software as a service* (*SaaS*). In addition, there are some other models, including *communication as a service* (*CaaS*) and *monitoring as a service* (*MaaS*).

Indeed, cloud computing provides dramatic benefits to organisations like companies and universities, such as lower cost, higher performance, productivity, reliability and scalability, and easier maintenance, but meanwhile it poses huge challenges to information security, including concerns in confidentiality, integrity and availability [2]. A precondition of solving these security problems is accurately registering every user's identity and strictly verifying it when the user is accessing the system in any way. Therefore, *identity management* becomes essential to security in cloud computing.

This paper will be discussing challenges which identity management in cloud computing environment faces as well as potential solutions. The rest of the paper will be organised as follows. Section 2 introduces the research context, including the concept of identity management and a number of practical identity management frameworks and systems. Section 3 discusses some important issues remaining in cloud identity management, and proposes some potential ideas to solve these problems. Section 4 concludes the paper.

II. CONTEXT

According to Oxford English Dictionary, the word *identity* is defined as "The quality or condition of being the same in substance, composition, nature, properties, or in particular qualities under consideration; absolute or essential sameness; oneness."

In computing context, an *identity* can be regarded a set of unique characteristics of an entity: an individual, a subject, or an object [3]. An identifier is an identity that is used for identification purpose [4].

Within a system, a user's identity must be unique so that the system can distinguish among different users. The *identification* process concerns the manner in which a user provides his unique identity to the system. However, one identity does not necessarily correspond to a single individual; multiple individuals may share an identity, probably during different time. Identification, together with *authentication*, is the fundamental process of information security, feeding information for access control.

A. Identity Managment

Identity management refers to the management of users' identities, answering questions such as whom they are, which privileges they have, what information assets they are allowed to access and in what manner, and so on. It would be rather important, as a computing system is normally supposed to be used only by those authorised, therefore unauthorised persons must be detected and excluded from the system; unauthorised access will damage the security of the system. Identity management sometimes can also be referred to as *identity and access management.*

According to Hamlen [5], in cloud computing environment, identity management is a trust model that handles (i) various trust relationships, (ii) access control policies based on roles and attributes, (iii) real-time provisioning, (iv) authorization, and (v) auditing and accountability.

B. Identity Management Systems

Identity management systems are information systems as well as technologies that are used to implement identity

978-1-4673-6850-6/15 $31.00 © 2015 IEEE
DOI 10.1109/ICISCE.2015.71

management strategies, policies, procedures and guidelines. Angin *et al*. [3] state that an identity management system supports the management of multiple digital identities. It also decides how to best disclose personally identifiable information to obtain a particular service.

There are a number of different kinds of identity management systems. According to Habiba *et al*. [6], identity management systems in cloud computing can be classified into four categories:

1) *Isolated identity management systems.* In such as system, a single server is used to provide services as a service provider; meanwhile it also stores and manages users' identification information [7]. Such a system does not rely on a trusted third party for the credential issuance and verification [8].

2) *Centralised identity management systems.* There are at least two servers in a centralised identity management system. At least one server is separated from service providers and is dedicated to the responsibilities of issuance, storage and management of identity data, while other servers are responsible for providing cloud services.

3) *Federated identity management systems.* Multiple organisations can use the same identity management system. The same identity credentials of subscribers from these organisations can be used to acquire access to all the networks within any particular trusted group of enterprises [9]. Such systems gain popularity due to their flexibility and scalability. They follow the distributed storage architecture, where identity information is stored at multiple locations [6].

4) *Anonymous identity management systems.* As the name implies, such a system does not disclose users' identity management information to others while doing authentication, it keeps users "anonymous" [10].

A number of practical identity management systems have been proposed and successfully developed.

Privacy and Identity Management for Europe [11] "aims to develop a working prototype of a privacy-enhancing Identity Management System". The PRIME architecture at a system level is comprised of parties that interact. A party may run an instance of the PRIME system allowing them to interact with other parties using PRIME protocols and to manage data they hold using PRIME technology. It is designed to support a comprehensive life-cycle management of identity-related data. It supports users to manage their identity data, in particular their (partial) identities.

Oauth [12] is "an open protocol to allow secure authorisation in a simple and standard method from web, mobile and desktop applications". It is a simple but rather safe and secure way to publish and interact with protected data. The protocol is flexible as it is adjustable to the actual security needs of different sites, and extensible through different signing algorithms and security features. On top of OAuth protocol, there is a simple identify layer called OpenID Connect [13].

User-Managed Access (UMA) is also based on OAuth, and it provides web-based access management. UMA allows resource owners to control their resources on whether they are allowed to be accessed by clients. The resources can reside on any number of resource servers. These servers use a centralised authorisation server to manage access to resources based policies set by resource owners [14].

ICEMAN, the abbreviation of Inter Cloud Identity Management, is an architecture for secure federated inter-cloud identity management. It aims to develop technical and organisational solutions for secure federated inter-cloud identity management. It attempts to leverage and integrate existing standards to foster quick service adoption [15].

As the scales of clouds become larger and larger, multiple clouds need to be federated to provide extensive services to users. Federated clouds pose new challenges to identity management due to their complicated distributed nature. A number of federated identity management systems have been proposed and implemented. Stihler *et al*. [16] proposed a new architecture for integral federated identity management system, aiming at IaaS users who wish to provide services and resources to other subjects. They introduced a new characteristic to translate high-level identities to lower-level identities in a transparent way, allowing authentication crossing the borders of separate clouds.

Before Stihler, Morgan *et al*. [17] introduced the Shibboleth approach to dealing with federated security, which was later used in cloud computing. The Shibboleth system includes two major software components: the Shibboleth Identity Provider (IdP) and the Shibboleth Service Provider (SP). These two components are deployed separately but work together to provide secure access to Web-based resources. It extends identity management for secure access to resources among multiple organisations.

Dhungana *et al*. [18] extends the CloNe architecture [19] by designing, deploying, and integrating an identity management framework customised for the CloNe infrastructure. It is based on the UMA protocol, supporting authentication, authorisation, and identity management of entities in the CloNe infrastructure and enabling federated identity management and management of access control policies across different infrastructure providers.

III. DISCUSSIONS

The above proposals and systems on identity management are working well and have solved some major problems appearing in cloud security. Some even have been working on federated environment. However, some issues are still worth further discussion and analysis.

Authentication is a fundamental process in identity management. There are a number of basic ways to achieve secure authentication, which can be combined to provide stronger authentication. With the rapid development of biometric technologies, biometric information can be used to authenticate users' identities. Meanwhile, cryptographic keys can also play a very important role in authentication. Public Key Infrastructure (PKI) is a good solution, as it combines a

user's identity with his public key using the private key of Certificate Authority, a kind of trusted third party, to sign the combined information. Although the above two technologies are relatively mature and widely supported, they have some disadvantages. Users must pre-register with the authority, and the information stored on certificate directories may disclose some critical personal and private information, which may raise concerns of some users.

This problem can be solved using Identity Based Cryptography (IBC) [20], where a user's public key can be derived directly from some unique identity information, such as biometric information or as simple as an email address. The development of IBC offers great flexibility and convenience while well protects users' privacy.

Heterogeneity is another big issue, especially in federated cloud environment, due to the potential heterogeneous nature of cloud computing. Different clouds may use different policies (or even different styles of policies), implemented using different languages on different platforms. Also, organisations use various ways to identify and authenticate users. Even the same user may have different identity information in these systems. It is difficult, but important, to break the borders of platforms and organisations, and make the identification and authentication process across platforms and organisations. To achieve this, some common languages should be used to describe the identity information as well as identity management policies.

IV. CONCLUSIONS

This paper has discussed the identity management issues within the cloud computing environment. Basic concepts of identity management have been introduced. Some identity management frameworks and systems have been introduced and analysed. Further discussions on the difficulties and issues of identity management in cloud have been done and a number of potential solutions have been given.

[1] S. Dhar, "From outsourcing to cloud computing: evolution of IT services", 2011 IEEE International Technology Management Conference (ITMC), San Jose, CA, USA, 2011.

[2] X. Ma, "Security concerns in cloud computing", Fourth International Conference on Computational and Information Sciences (ICCIS), Chongqing, China, 2012.

[3] P. Angin, B. Bgargava, R. Ranchal, N. Singh, and M. Linderman, "An entity-centric approach for privacy and identity management in cloud computing", 29th IEEE International Symposium on Reliable Distributed Systems, New Delhi, India, 2010.

[4] A. Josang, and S. Pope, "User centric identity managemen", Proceedings of AusCERT, Gold Coast, 2005.

[5] A. Hamlen, P. Liu, M. Kantarcioglu, B. Thuraisingham, and T. Yu, "Identity management for cloud computing: developments and directions", Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, Oak Ridge, TN, USA, 2011.

[6] U. Habiba, A. G. Abassi, T. Masood, M. A. Shibli, "Assessment criteria for cloud identity management systems", IEEE 19th Pacific Rim International Symposium on Dependable Computing, Vancouver, British Columbia, Canada, 2013.

[7] Y. Cao, L. Yang, "A survey of identity management technology", IEEE 2010 International Conference on Information Theory and Information Security (ICITIS), Beijing, China, 2010.

[8] A. Josang, J. Fabre, B. Hay, J. Dalziel, S. Pope, "Trust requirements in identity management", Proceedings of the 2005 Australasian Workshop on Grid Computing and E-Research, Volume 44. Australian Computer Society, Inc., 2005.

[9] S. Suriadi, E. Foo, A. Josang, "A user-centric federated single signon system", Journal of Network and Computer Applications, 32(2):388–401, 2009.

[10] A. Bhargav-Spantzel, J. Camenisch, T. Gross, D. Sommer, "User centricity: a taxonomy and open issues", Journal of Computer Security, 15(5):493–527, 2007.

[11] PRIME, https://www.prime-project.eu, 2004.

[12] OAuth, http://oauth.net, 2007.

[13] OpenID Connect, http://openid.net, 2007.

[14] UMA, https://tools.ietf.org/html/draft-hardjono-oauth-umacore-10, 2014.

[15] G. Dreo, M. Golling, W. Hommel, F. Tietze, "ICEMAN: An architecture for secure federated inter-cloud identity management", 2013 IFIP/IEEE International Symposium on Integrated Network Management, Ghent, Belgium, 2013.

[16] M. Stihler, A. O. Santin, A. L. Marcon, J. S. Fraga, "Integral federated identity management for cloud computing", 5th International Conference on New Technologies, Mobility and Security (NTMS), Istanbul, Turkey, 2012.

[17] R. L. Morgan, S. Cantor, S. Carmody, W. Hoehn, K. Klingenstein, "Federated security: the Shibboleth approach", EDUCAUSE Quarterly, 27(4):12-17, 2004.

[18] R. D. Dhungana, S. Rangarajan, A. Mohammad, A. Sharma, I. Schoen, "Identity management framework for cloud networking infrastructure", 9th International Conference on Innovations in Information Technology (IIT), Abu Dhabi, United Arab Emirates, 2013.

[19] P. Murray, D-5.2 (D-D.1) Cloud Network Architecture Description, European Commission's 7th Framework Program, Tech. Rep., 2011.

[20] D. Bonhe, M. Franklin, "Identity-based encryption from the Weil pairing", Advances in Cryptology – CRYPTO, Springer, 2001.