ENHANCING THE SECURITY FRAMEWORK SECURECLOUD WITH THE SWIFT IDENTITY MANAGEMENT FRAMEWORK

Abdulrahman H. Altalhi[1], Zailani Mohamed Sidek[2], Norjihan Abdul Ghani[3], Fazidah Othman[4] and Maged Abdelkhaleq Al-Sheshtawil[5]

[1]Department of Information Technology, Faculty of Computing and IT, King Abdulaziz University Jeddah, Saudi Arabia

ahaltalhi@kau.edu.sa

[2]Information Security Department, Advanced Informatics School (AIS), Universiti Teknologi Malaysia, 54100 Kuala Lumpur, Malaysia

zailani@utm.my

[3]Information Systems Department, Faculty of Computer Science & Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia

norjihan@um.edu.my

[4]Department of Computer System & Technology, Faculty of Computer Science & Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia.

fazidah@um.edu.my

[5]Information Technology Department, College of Computing & IT, King Abdul Aziz University, Jeddah, Saudi Arabia

malsheshtawy@kau.edu.sa

ABSTRACT

SecureCloud is a comprehensive security framework for cloud computing environments consisting of different modules that handle the security and trust issues of key components. One of the modules is responsible for authentication and identity management (IDM). In SecureCloud, the author suggest, to implement the security solution for the Authentication and IDM module, it is important to ensure IDM services in the cloud can be integrated with the existing IDM framework. Existing techniques for use of pseudonyms and accommodating multiple identities to protect users' privacy can help build a desired user-centric federated IDM for clouds. Motivated by attempting to find a solution from the suggestion, this paper proposes the integration of SWIFT identity management framework into the module using the existing trust relationships in SecureCloud to enhance the security of the SecureCloud framework. SWIFT provides a set of advanced security features such as identity aggregation, privacy protection, advanced access control and single sign-on (SSO) to help enhance the security of IDM module in SecureCloud.

KEYWORDS

Security framework, cloud computing, authentication, identity management, security.

DOI : 10.5121/ijccsa.2012.2101

1. INTRODUCTION

Research in cloud computing has recently gained tremendous momentum in both the academic and industrial communities. Cloud computing has grown in existing computing technologies through modules such as Software as a Service (SaaS), Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) and each of these services has its own security issues. Although security issues are delaying its immediate adoption, cloud computing appears to be an unstoppable development, and we should attempt to provide reliable mechanisms for its secure adoption.

Surveys of potential adopters indicate that security and privacy are the primary concerns hindering the adoption of cloud computing [1]. Furthermore, most cloud computing research focuses on security issues [2, 3, 4, 5, 6] and attempts to provide a vision and roadmap for the direction of future research. With the exception of CloudSim [7] and well-known cloud computing infrastructures such as Microsoft Azure [8], Amazon EC2, Google App. Engine, and Aneka [9], there are few frameworks being developed to enable secure adoption in a cloud environment. Due to limited resources, Hassan, James and Gail-Joon Ahn [10] collaborated to develop a comprehensive security framework for the cloud computing environment called SecureCloud. In the next section, we briefly describe this framework, which consists of different modules handling security and trust issues of key components such as identity management and access control. Regardless of which features and properties for securing a cloud environment are provided, the security solution they suggest is too general and not detailed in terms of implementation. Motivated by attempting to find a solution, we will describe one of the most important modules, Authentication and Identity Management, in detail, and propose a solution to enhance the security of this framework.

2. SecureCloud FRAMEWORK

The framework consists of different modules to handle security and trust issues in key components of cloud computing environments such as identity management, access control, policy integration among multiple clouds, trust management between different clouds, trust management between a cloud and its users, secure service composition and integration, and semantic heterogeneity among policies from different clouds.

2.1 Key Components

The overall security framework and the key components of the cloud computing environment are depicted in Figure 1. The *Services Integrator* facilitates collaboration among different service providers by composing new desirable services. Each service integrator has components that are responsible for establishing and maintaining trust between local provider domains and between providers and users. They also provide the services desired by users and generate global policies. The service integrators first discover services from different service providers or other service integrators and then carry out negotiations, integrate the services to form groups of collaborating services and provide them to users [10].

The security management component provides the security and privacy specification as well as the enforcement functionality, while the authentication and identity management module is responsible for authenticating users and services based on credentials and characteristics. In the service provider, the access control module employs the access policies, while the privacy and data encryption module is responsible for privacy standards and encryption of outsourced data. In the service integrator, the trust-based policy integration (TPI) module is the key component that administers and facilitates trust-based policy integration among different services from different service providers.

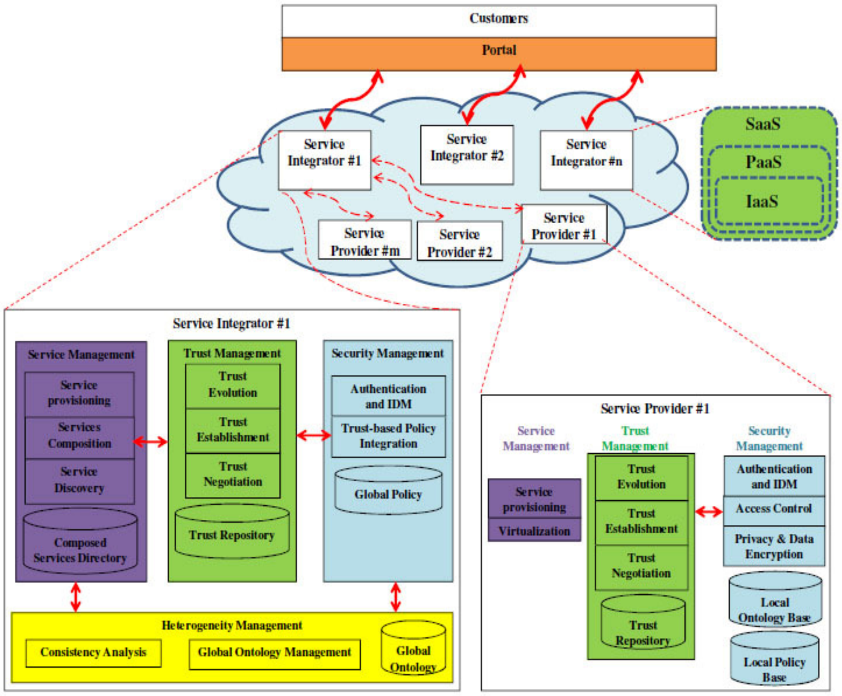

Figure 1. Security Framework for Cloud Computing Environments (Source: [10])

The service management component is responsible for secure service discovery, composition and provisioning, and the service provider uses virtualization to offer these services to users. Next, the service discovery module is responsible for finding different services that provider domains or other service integrators offer. After discovering the services, the service integrator must negotiate with provider domains to compose new collaborating services that are desired by users using the service composition module. The collaborating services come from different domains, however, and the service integrator must consider the trust between the collaborating provider domains when composing new services. The service provisioning module provides services for users based on bidirectional trust between the service integrator and its users. The trust management module is responsible for the negotiation, establishment, and evolution of trust. The global ontology management module provides global ontology and supports semantic heterogeneity related to policies. Finally, the consistency analysis module checks the correctness of the integrated policies [10]. For further readings on this framework, please refer to [10]. Next, we will elaborate on the Authentication and Identity Management module to show the importance of this module.

2.2 Authentication and Identity Management Module

Users can easily access their personal information using cloud services and the authentication and identity management module is also available for various services across the Internet. The Identity management (IDM) mechanism is used to authenticate users and services based on their credentials, profile, and/or characteristics [11]. A potential problem area with IDM in the cloud concerns the interoperability issues that may result from the use of different identity tokens and different identity negotiation protocols. An IDM system should be able to accommodate privacy concerns for the protection of private and sensitive information associated with users and processes.

In relation to interoperability problem mentioned above, user-centricity is an essential characteristic for providing flexible, scalable IDM service. User-centric IDM has recently received significant attention for handling private and critical identity attributes [12]. In this approach, an identity has identifiers or attributes that identify and define each user. The user-centric approach allows users to control their own digital identities and also takes away the complexity of IDM from the enterprises, allowing users to focus on their own functions. Based on the approaches given, it is desirable to have a functional scheme to handle the authentication process and manage IDM.

3. METHODOLOGY

In SecureCloud, the author suggest, to implement the security solution for the Authentication and IDM module, it is important to ensure IDM services in the cloud can be integrated with the existing IDM framework. Existing techniques for use of pseudonyms and accommodating multiple identities to protect users' privacy can help build a desired user-centric federated IDM for clouds. Based on this suggestion, we went through SWIFT IDM framework.

3.1 SWIFT Identity Management Framework

SWIFT specifically aims to provide the user with the required mechanisms to utilize identity information with any service accessed, whether it is a web service or the network access service. In addition to its cross-layer view of identity management, SWIFT also provides a set of advanced topics such as identity aggregation, privacy protection, advanced access control and single sign-on (SSO) [13]. These topics focus on usability from a user-centric perspective, and these features match the SecureCloud framework. SWIFT is an identity management framework [14] that allows users to link their existing subscriptions with the service and with identity providers into virtual identities, and SWIFT then allows users to make use of these virtual identities to request service access. In this context, a virtual identity is the aggregation of identity information (i.e., attributes and credentials) coming from different identity providers and identified by a virtual identifier. Users make use of these virtual identifiers to gain access to services that are provided after taking into account the information that was aggregated into the specific virtual identity. Additionally, the use of virtual identities provides the end user with the possibility of performing a single sign-on between services, even if they are located in different Open Systems Interconnection (OSI) layers (cross-layer single sign-on). In this way, the framework controls user access.

3.2 SWIFT Features

- Virtual Identities

A virtual identity is a special kind of digital identity that is the aggregation of attributes and credentials from different sources (providers). The virtual identity does not contain actual aggregated data; rather, it contains references to the information in its original source. Each virtual identity is identified by a unique virtual identifier. As virtual identities are used to access services, end users only need to remember the credentials that have been aggregated into the generated virtual identity. Additionally, as information is referred to virtual identities rather than copied, an attribute value that is modified or deleted from its original source has an immediate effect on the services accessed using a virtual identity.

A virtual identity (Figure 2) contains a reference to authentication credentials, including the provider identifier, with responsibility over the end user authentication credentials (authentication provider) and an end user identifier. It may also contain references to attributes provided by attribute providers. These are similar to the authentication attributes but also include the name of the attribute [15].

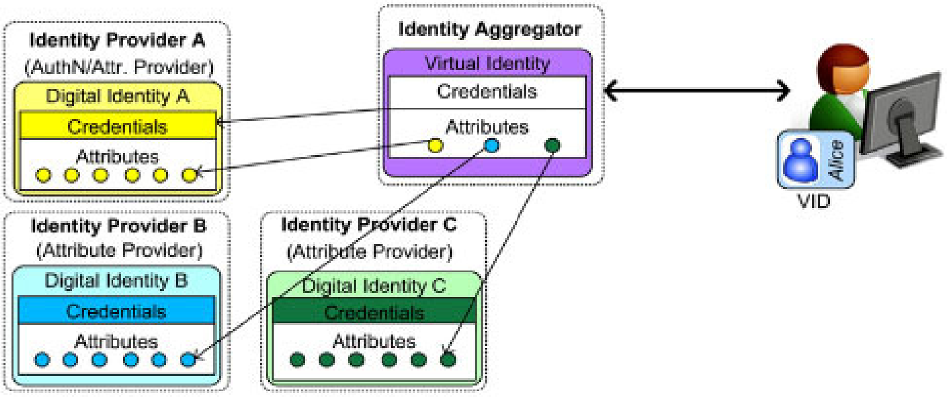

Figure 2. Virtual identity concept and relation among providers.

This module can, therefore, be included inside the Authentication and Identity Management module in SecureCloud. The new framework is depicted in Figure 3.

- Properties

To provide certain functionalities, several considerations must be taken into account.

- Functional properties

  • Virtual Identities. Users are able to create as many virtual identities as they want.
  • Single Sign-On (SSO). The framework provides SSO to avoid requiring the end user to re-authenticate each time access to a protected service that makes use of the same validity period is requested.
  • Cross-layer. SSO allows end users to authenticate themselves with protected services at the same or different layer from the one that was first authenticated (network and application layers).
  • Authorization and access control. The framework provides the mechanism to ensure an advanced access control process where service providers can make decisions based on end user attributes (role, entitlement, etc.), in addition to authentication statements.

- Security properties

  • Authentication. End users can access services through one of their virtual identities. Services are also able to obtain end user attributes from these virtual identities to perform authorization tasks. As for authentication methods, end users authenticate with each provider involved during the creation of virtual identities and are able to use several methods that depend on the layer in which the authentication is first

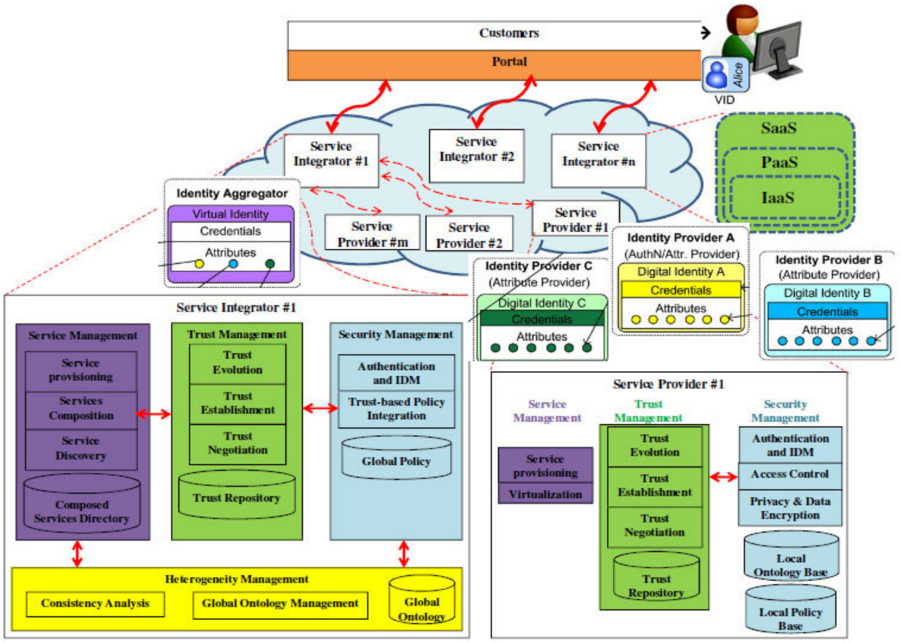

Figure 3. SecureCloud Framework with the SWIFT IDM Module

performed. Impersonation by other end users or entities should be avoided, except by those previously authorized by the end user.

• Privacy. To achieve end user privacy, end users are able to control the release of their attributes depending on the specific services utilized, and this is performed by attribute release policies. In addition, service providers are not able to determine who the end user actually is from the information they receive. That is, the end user accesses can be hidden from certain entities. However, mechanisms exist to determine a user's identity and to provide irrefutable proof of his or her actions, if necessary.

• Linkability. The framework provides some level of unlinkability from the service provider perspective. Specifically, different accesses to protected services using the same virtual identity may be delinked, if so desired. Moreover, two different virtual identities are not linkable to each other.

For further information on the properties and framework entities of SWIFT, please refer to [15].

Integrating the SWIFT IDM framework into the Authentication and Identity Management module in SecureCloud, let us have additional security features such as identity aggregation, privacy protection, advanced access control and single sign-on (SSO). These features are especially important for handling private and critical identity attributes.

4. CONCLUSION

Cloud computing is new and growing very quickly, but because security issues are still delaying its adoption, we need to provide security mechanisms to ensure that cloud computing benefits are fully realized and utilized. Cloud computing has profound implications not only for Internet services but also for the information technology sector as a whole. Although there are many advantages to using a cloud-based system, practical problems remain that have to be solved before the technology can be more fully deployed, particularly those problems related to service-level agreements, security, privacy, and power efficiency. As described in this paper, unsolved security problems still prevent many potential users from engaging in cloud computing. Until the proper security mechanisms are put in place, potential users will not be able to leverage the advantages of this technology. This security module should cater to all of the issues arising from all directions of the cloud, be it a SaaS, IaaS or PaaS service module. SecureCloud is a good example of a comprehensive security framework, and integrating this framework with other modules will raise cloud computing to another level of security.

References

[1] P.J. Bruening and B.C. Treacy, (2009), “Cloud Computing: Privacy, Security Challenges,” Bureau of National Affairs, www.hunton.com/files/tbl_s47Details/FileUpload265/2488/CloudComputing_Bruening-Treacy.pdf.

[2] Balachandra R.K., Ramakrish P.V. and Atanu Rakshit, (2009), “Cloud Security Issues”, Proceeding Of IEEE International Conference on Services Computing, IEEE.

[3] Cloud Security Alliance. Security best practices for cloud computing. /http://www.cloudsecurityalliance.org [accessed on 10 April 2010].

[4] Tsai W, Jin Z, and Bai X., (2009), “ Internetware computing: Issues and perspective”, Proceedings of the 1st Asia-Pacific Symposium on Internetware, Beijing, China, ACM, pp. 1–10.

[5] Subashini S. and Kavitha V., (2010), “A survey on security issues in service delivery models of cloud computing”, Journal of Network Computing and Application, Vol. 7, No. 6.

[6] Dorey P.G. and Leite A., (2011), “Commentary : Cloud computing: A security problem or solution?”,
Information Security Technical Report.

[7] Calheiros, R.N. et al., (2009), “CloudSim: A Novel Framework for Modeling and Simulation of Cloud Computing Infrastructures and Services”, Proc. Of the 38th International Conference on Parallel Processing, Vienna, Austria, 22-25 September 2009. IEEE Computer Society.

[8] D. Chappell, (2008), “Introducing the Azure services platform”, White paper, Oct. 2008.

[9] X. Chu et al., (2007),“Next-generation enterprise grid platform for e-science and e-business applications”, Proceedings of the 3rd IEEE International Conference on e-Science and Grid Computing.

[10] Hassan Takabi, James B. D., Joshi and Gail-Joon Ahn, (2010), “SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments”, Proc. of the 34th Annual IEEE Computer Software and Applications Conference Workshops, IEEE.

[11] Elisa Bertino, Federica Paci and Rodolfo Ferrini, (2009), “Privacy-preserving Digital Identity Management for Cloud Computing”, IEEE Computer Society Data Engineering Bulletin, pp. 1-4.

[12] Moonam Ko, Gail-Joon Ahn and Mohamed Shehab, (2009), “Privacy Enhanced User-Centric Identity Management”, Proceedings of IEEE InternationalConference on Communications, Dresden, Germany, June 14-18, 2009.

[13] R. Semancik, (2005), “ Internet Single Sign-On Systems”, nLight, Research Report.

[14] G. Lopez, O.C. Reverte, A.F. Gomez-Skarmeta and J. Girao, (2009), “A SWIFT take on Identity Management”, IEEE Computer Vol.42, No.5, pp. 58–65.

[15] Alejandro Pérez et al., (2011), “Formal description of the SWIFT Identity Management Framework”, Journal of Future Generation Computer Systems, Vol. 27, pp 1113–1123.