Chapter 16
An Extensible Identity Management Framework for Cloud-Based E-Government Systems

Hirra Anwar
National University of Sciences and Technology (NUST), Pakistan

Muhammad Awais Shibli
National University of Sciences and Technology (NUST), Pakistan

Umme Habiba
National University of Sciences and Technology (NUST), Pakistan

ABSTRACT

Numerous Cloud Identity Management (IdM) systems have been designed and implemented to meet the diverse functional and security requirements of various organizations. These requirements are subjective in nature; for instance, some government organizations require security more than efficiency while others prioritize performance and immediate response over security. However, most of the existing IdM systems are incapable of handling the user-centricity, security & technology requirements and are also domain specific. In this regard, this chapter elaborates the need to use Cloud Computing technology for enhancing the effectiveness and transparency of IdM functions and presents a comprehensive and well-structured Extensible IdM Framework for Cloud based e-government institutions. We present the design and implementation details of the proposed framework, followed by a case study which shows how government organizations of Pakistan would use the proposed framework to improve their IdM processes and achieve diverse IdM services.

INTRODUCTION

With the increase in development and deployment of SaaS (internet based Software-as-a-Service) applications, the demand and significance of digital identity has taken a whole new dimension (Van, 1989). Identity being the key component of many services including e-commerce, e-business and e-healthcare

DOI: 10.4018/978-1-5225-0159-6.ch016

has evolved with the evolution in the field of information technology and industry. Furthermore, modern technologies such as Cloud, has also offered cutting-edge solution by presenting various Identity Management (IdM) solutions including the concept of Identity-as-a-service (IDaaS) to organizations and customers (Emig, 2007). These IdMSs, besides providing basic IdM services, offer all of the Cloud benefits, such as reduced hardware cost and easy management with wide range of integration options (Subashini, 2011; Rimal, 2009). As a result of this, most of the organizations are moving their existing enterprise IdMSs to Cloud based services.

Numerous efforts have been dedicated to the field of Cloud IdM to meet the dynamic and multi-dimensional user requirements (security and functionality); however, offering a comprehensive and secure IdM system is still a daunting challenge. In addition, since security and functionality requirements vary from organization to organization, most of the Cloud providers have to implement their own custom IdM solutions. Undoubtedly, customized IdM solutions adhere to the desired functionality and security requirements; however these systems generally are not flexible enough to satisfy the changing business and security requirements. In addition to this, regardless of various advantages including controlled access, improved user experience and efficiency; implementing a secure, extensible & generic IdM system involves high cost, liability, risk, legal compliance and many other significant challenges (Subashini, 2011; Maler, 2008).

For-instance, for any small or medium sized organization, isolated IdM system might seem to be an attractive solution in the beginning, however, with the growth and expansion in business, requirements for security and functionality may change as well. For example, at a later point that organization may desire to distribute its sensitive identity information across multiple servers for security reasons or share them with other partner organizations for enhanced functionality. Ideally, for such scenarios, Federated IdM is the applicable solution that facilitates secure sharing and distribution of identity credentials across multiple Cloud servers/domains. However, flexibility of interchanging one IdM solution with other, as a matter of fact is typically not supported in any of the existing solutions. Therefore, existing IdM systems become incapable to meet the scalable and flexible organizational requirements.

Other than flexibility, cloud based IdM systems face technological and security challenges. Due to the rapid advancement in technology and increase in federation of web services, IdM operations are required to be standardized. Standards are well-known for defining common set of procedures, semantics, and working principles that allow various components of an IDMS to collaborate. The task of standardization is taken up by various authoritative organizations including *Kantara Initiative* (Liberty Alliance, 2002), *OASIS* (Federation, 2011) and *ITU-T* (Telecommunication Standardization Sector) (Sarma, 2009). In addition to this, IdM industry is also continuously working on developing new protocols and initiating various pilot projects. These projects and protocols are primarily targeted at facilitating IdM services. Further, in the related work section, we present a comprehensive list of widely accepted projects and protocols including *PRIME, Shibboleth, OpenID, OAuth* etc. and highlight their features along with similarities and differences.

Besides the inherent identity security issues such as ensuring confidentiality, integrity, availability, privacy, and secure IdM, the association of Cloud computing has introduced numerous other security challenges to this paradigm. These issues mainly include lack of transparency, secure logging, limited disclosure and synchronization among many others. It is because of these issues that Cloud service consumers usually demand to have maximum control over the sharing and distribution of their sensitive identity information. As another logical outcome of these security challenges, cloud service providers are required to invest more time, effort and money in designing and developing secure and privacy