A Secure Mobile Cloud Identity: Criteria for Effective Identity and Access Management Standards

Nitin Naik and Paul Jenkins
Defence School of Communications and Information Systems
Ministry of Defence, UK
Email: nitin.naik100@mod.uk and paul.jenkins683@mod.uk

***Abstract*—Managing digital identities and access control for cloud users and applications remains one of the greatest challenges facing cloud computing today. This led to a new cloud security service paradigm called identity and access management (IAM) service, IDentity-as-a-Service (IDaaS). Many IAM standards have been proposed in the last two decades: Lightweight Directory Access Protocol (LDAP), Central Authentication Service (CAS), OZ Protocol, Security Assertion Markup Language (SAML), CoSign Protocol, Open Authentication (OAuth), and OpenID Connect (OIDC). However, Mobile Cloud Computing (MCC) IAM requirements are somewhat different due to its resource limitations and mobile communication. It may not be necessary that the same IAM standards are equally effective for MCC. To determine the appropriateness of these IAM standards for MCC requires some IAM performance evaluation criteria. Therefore, this paper proposes several evaluation criteria for an effective IAM standard for MCC.**

Keywords*—*Identity and Access Management, IAM, Mobile Cloud Computing, MCC, IDaaS, SSO

I. Introduction

The amalgamation of cloud computing, mobile devices, wireless infrastructure, mobile web, and location-based services delivers a new computing paradigm called Mobile Cloud Computing (MCC) [1]. In MCC, the authentication and authorization task across the domains, organisations, and clouds is a complex task [2]. Every delivery platform and service model requires different authentication and authorization measures. In one particular scenario, it is possible that consumers or users hold multiple accounts with service providers such as Google, Amazon, e-Bay, and AOL. The visibility and scope of attributes for every identity have to be verified against a central trusted policy framing authority, assumed by the systems [3]. The most common cloud-based solution to this complex situation is Identity and Access Management (IAM), which offers the right access to the right user at the right time for the right reasons.

One of the important aspects of IAM is the current IAM standards and their strengths and limitations. There are various IAM standards that have been proposed over the last two decades: LDAP, CAS, OZ, SAML, CoSign, OAuth and OIDC. However, mobile cloud computing IAM requirements are rather different because it is based on resource optimisation with small devices. Despite the success of MCC, it has its inherent challenges of mobility, resource scarcity, heterogeneity, and insecure wireless communication [4]. Based on its limitations, mobile cloud users need strong, extensive and lightweight security mechanisms for the authentication and authorization [5]. It should support both web applications, native mobile applications, consumers and enterprise environments [6]. This list may be longer depending on the choice of MCC delivery platforms and service models. The crucial questions are that how many IAM performance evaluation criteria are enough for MCC and whether the existing IAM standards are suitable for MCC or not? Therefore, this paper proposes several evaluation criteria for an effective IAM standard for MCC.

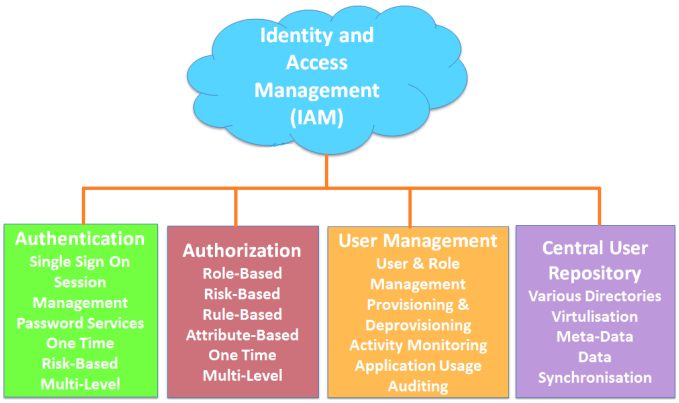

Fig. 1: Identity and Access Management (IAM) Components

II. Identity and Access Management Evaluation Criteria for Mobile Cloud Computing

A. Extensive Authentication and Authorization Support

In MCC, user identity and access control has to be managed across all the types of cloud delivery models (public, private and hybrid) and service models (SaaS, PaaS and IaaS) over on the wireless medium. Every delivery platform and service model requires different authentication and authorization measures. This can be accomplished using a one-time, certificate-based, risk-based, multi-factor, and multi-level authentication and authorization technique. Therefore, a generic IAM standard is required that can accommodate all the mobile cloud models and include a wide range of attributes, identifications and access mechanisms.

B. User-Friendly Single Sign-On Support

Mobile cloud has a plethora of services and apps and access to them needs separate authentication. This requirement causes several issues such as memorising numerous passwords, frequent login to the same service or app, frequent password change, phishing, and password recovery. Consequently, this affects the overall performance and productivity of the organisation. SSO can solve this issue by offering a centralized,

secure, convenient, and user-friendly method of authenticating a user one time within an environment. An IAM standard must not only support the SSO functionality but also provides a user-friendly sign-on approach for small devices.

C. Lightweight Standard/Protocol

A mobile cloud IAM standard should be a lightweight standard/protocol for over-the-air mobile applications. They tend to have lesser overall size, leave out unessential data and might use a data compression technique to have a lighter effect on network communication [5]. It is simpler, faster and easier to manage than other communication protocols used on a local or wide area network. Therefore, it is one the greatest requirements of an IAM in MCC.

D. Platform Independent, Vendor-Neutral and Open Standard

Mobile cloud computing is a heterogeneous environment, which includes diverse platforms, applications, services, vendors and IT infrastructures. It is an amalgamation of a mobile environment, desktop environment, and many more environments; therefore an IAM standard should be an open, platform independent, vendor-neutral, industry standard to provide operability in every environment.

E. Scalable Standard

There is always balanced to be achieved between security and scalability. However, the rapid escalation in mobile cloud computing market has been demanding for scalable standards to cope with the increasing number of users, services and resources. Therefore, an IAM standard should be capable of incorporating increasing users, consumers, resources and apps without affecting cost, performance, and security.

F. Web and Native Mobile Apps Support

Mobile cloud applications are a fusion of applications developed using native platform language and hybrids, which is a blend of HTML5 and native language. However, mobile browsers may be more constrained in the maximum URL length they support. Moreover, WebView has a number of limitations such as preventing the sharing of cookies, certificates, and HTML5 local storage. This highlights the two different types of mobile cloud apps and their different requirements. Therefore, an IAM standard should support both types of apps as well as cross-linking between them.

G. Consumer and Enterprise Support

Mobile cloud supports various business models such as enterprise-to-enterprise, enterprise-to-consumer, or within an enterprise. The authentication and authorization requirements are completely different for different models. Therefore, an IAM standard should support at both enterprise and consumer levels.

H. Immediate Revocation of Access Support

Security threats happen more often on mobile devices than desktop PCs. They are more likely to be lost and more likely to be shared with someone else. Consequently, an immediate revocation support is equally important similar to an appropriate grant support. Administrator or user should be able to revoke the access anytime when these things happen. This must be the part of any successful IAM standard.

I. End User Delegated Authorization Support

In MCC, many apps and services share data and resources to improve speed and productivity in addition to user experience. However, this functionality requires continuous interaction between them and may require a delegation on behalf of a user. This is one of the most innovative features for mobile users to avoid frequent authorization to apps and services. Therefore, any IAM standard developed for mobile users should support this feature.

J. Data Integrity Support

Mobile cloud computing has the biggest challenge of open and insecure wireless communication, which is prone to eavesdropping attacks. The security tokens transported over wireless channels have not been tampered with or altered over its entire life cycle. An IAM standard must incorporate the strong digital signature or MAC to maintain the integrity of authentication and authorization tokens.

K. Data Confidentiality Support

Insecure wireless communication can also affect or limit the ability of mobile cloud system to protect the sensitive information of security tokens from disclosure to unauthorized parties. An IAM standard must incorporate the strong encryption technique to ensure the confidentiality of information in the security tokens in MCC alongside with minimizing the processing overhead on mobile devices.

L. Mobile Standard

One of the major differences between MCC and other types of cloud computing is the substantial use of mobile devices. Consequently, authentication and authorization also rely on typical mobile entities, protocols and standards. Many IAM standards may be suitable for mobile devices but may not be very effective. Therefore, an IAM standard should incorporate mobile standards or provide a dedicated version for the mobile devices.

III. Conclusion

This paper has proposed several identity and access management (IAM) performance evaluation criteria to determine an effective IAM standard for MCC. In future, it would be interesting to perform a practical investigation for popular IAM standards based on the proposed IAM performance evaluation criteria.

References

[1] A. N. Khan, M. M. Kiah, S. U. Khan, and S. A. Madani, "Towards secure mobile cloud computing: A survey," *Future Generation Computer Systems*, vol. 29, no. 5, pp. 1278–1299, 2013.

[2] C. A. Gunter, D. Liebovitz, and B. Malin, "Experience-based access management: A life-cycle framework for identity and access management systems," *IEEE Security & Privacy*, vol. 9, no. 5, p. 48, 2011.

[3] A. Gopalakrishnan, "Cloud computing identity management," *SETLabs briefings*, vol. 7, no. 7, pp. 45–55, 2009.

[4] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[5] M. R. Momeni, "A lightweight authentication scheme for mobile cloud computing," *International Journal of Computer Science and Business Informatics*, vol. 14, no. 2, 2014.

[6] Pingidentity.com. (2011) A standards-based mobile application idm architecture. [Online]. Available: http://www.enterprisemanagement360.com