Limitations and Constraints in the Current Federated Access Management Systems

Sara J. Alotaibi, Dr. Mile Wald, Lester Gilbert, *ECS, University of Southampton*

***Abstract*—The increasing needs for updated information and collaborations around the world initiates the need to integrate Access Management Systems (AMSs) with each other. The integration of AMS developed the concept of Federated Access Management Systems (FAMSs). However, even this development was not able to cease the need for maintaining multiple accounts; it could only reduce the need. Moreover, the existing AMS and FAMS do not provide the security and privacy desired; these systems tend to have trust, identification and biased services issues related to them. Along with these performance issues, a lack of personalisation, usability and accessibility issues also reside. Furthermore, following extensive analysis of the current systems, a new term has been invented for an innovative system which will address the limitations and constraints of FAMS—Ubiquitous Access Management Systems (UbAMSs).**

***Index Terms*— Access Management Systems, Federated Access Management Systems, Ubiquitous Access Management Systems**

I. Introduction

The internet has played a great role in the evolution of modern lifestyles, and the development of the 'Web' had made the internet more accessible and more convenient to its users. Different services started being offered on the web which has created the need for the users to create online accounts, which requires the entry of personal information and details. Another aspect which has threatened information revolves around the fact that organisations made their customers' data available on the internet so that their services could be available online; however, the availability of an ocean of knowledge and personal information tempted malicious users to utilise such personal data for criminal purposes, and different techniques were invented to threaten the privacy of the users.

The violation of user privacy created a daunting need for rights management systems which would be able to authenticate the users [1, 2]. AMSs provided access rights for a specific system only to the users whose identity could be verified by the system [3, 4]. This was a major improvement with respect to the issue of security breaches of personal details and identity attributes. However, AMSs at this time were lacking in the area of providing unified access across several systems; these systems provided identity management to single systems or organisations [5], [6]. The constraint of limited access and the maintenance of multiple accounts for accessing different organisations did not meet the highly competitive needs of the modern world. Therefore, FAMSs were created with the aim of providing access to several systems and organisations through a unified identity [7], [8]. Importantly, FAMSs reduced the need to maintain several accounts, and also facilitated the tracking of the data revealed on the web. Notably, it is very common for individuals to forget the information that is given at the time of registration for different accounts and services. FAMSs provide a single domain for the provision of access to several accounts; therefore, information was maintained only on a single source.

The paper is structured in the following manner; Firstly, the background of the subject, including a brief overview of the exstsing FAMS are explained in *Section 2*. This is followed by a critical review of existing FAMS with various different criteria in *Section 3*. Finally, *Section 4* concludes the paper with a summary and proposes a new solution, UbAMS.

Sara. Jeza Alotaibi , Postgraduate, full-time research in Web and Internet Science and Electronic, University of Southampton, UK. (e-mail: sja2g09@ecs.soton.ac.uk).

Dr Mike. Wald, Academic staff in Web and Internet Science, University of Southampton, UK. (e-mail: mw@ecs.soton.ac.uk).

Lester Gilbert , Academic staff in Electronic and Software Systems, University of Southampton, UK. (e-mail: lg3@ecs.soton.ac.uk).

II. Federated Access Management Systems (FAMS)

The Federated Access Management System has been an area of attention for a few years for various different organisations. Accordingly, many systems have been developed including;

A. *Liberty Alliance Project*

It provides a platform for the users to perform their online transactions in a secure manner. The identities of the users are federated therefore greater access can be achieved [23], [11], [24].

B. *Shibboleth*

It is an open source website that provides the facility of single sign-in service to the customers [11], [14], [15]. It offers access to the internal as well as external content of the organisation [22], [21].

C. *OpenSSO*

It offers single sign-in service across different domains to save the user from the trouble of resetting forgotten passwords that proves to be a tedious process for the organisation if many users initiate it [8], [9].

D. *OpenID*

It is a single sign-in service for the maintenance of multiple accounts. It provides the service of even registering at any website with the credentials provided at OpenID, on user's request [11], [12], [21], [13].

E. *FingerID*

It also offers the maintenance of multiple accounts and a viewing facility on a single platform. However, FingerID offers greater accessibility and convenience owing to

fingerprint recognition and user-friendly displays, respectively [11], [25], [30].

The FAMSs claim to provide access over numerous sources and give the facility of single sign-in. Even though there exists a limitation amongst these applications and systems, the user still uses various different identities for every federated system: for example, an OpenID account and identity will not work for Shibboleth services. Furthermore, different applications offer different services; as such, the user might make accounts on multiple systems. This will again raise the need to remember multiple passwords. It can be stated that there is no single sign-in service or federated access across all federated access management systems. The FAMSs provide access to their respective specific set of domains; therefore, the user will create different accounts in order to gain access to the domains which are not accessible by a certain federated access management system [9], [10]. Other aspects of FAMSs which constrain its usage include the lack of usability and accessibility features in most of the federated access management systems. The systems should not only be federated with respect to the access with different systems, but also federated with regard to the different needs of the people who use them.

III. Analysis of FAMS

The FAMSs are evaluated with respect to various different criteria; the major classifications of the criteria are the different factors of FAMS [29] and Accessibility/Usability aspects of the system. The criteria of analysing the effectiveness of a federated access management system includes various different factors, as highlighted below.

A. *Trust (T):*

American Heritage defines the term 'trust' as the "confidence in terms of the integrity and capability of a thing or person" [26]. Customers trust the access management system to safeguard their data; accordingly, the data has to be protected to the extent that it should not even be forwarded via an unreliable intermediate source.

B. *Security (S):*

The term 'security' can be defined as the "freedom of danger or risk of any sort" [26]; therefore, only authorised parties are permitted access to the data in order to enforce security in AMS [27].

C. *Privacy (P):*

Privacy can be defined as the right of the individual to keep his possessions or data safe from others [26]. In this regards, users enter different forms of information in the access management systems, such as email addresses, login credentials for web accounts, etc. Notably, it is the responsibility of the access management system to ensure that this information is not exposed to any third party [27].

D. *Neutrality (N):*

Neutrality can be defined as the instance when no sides are being supported; rather, an equal share is given to all [54]. All systems and organisations should be dealt with according to the same scale, and no service or organisation should be given greater priority in terms of the utilisation of resources.

E. *Identity (I):*

Identity is defined as the "collective aspect of something by which it can be recognised" [26]. The credentials should be able to identify the individuals in a reliable and effective manner.

F. *Languages (L) and Culture (C):*

Culture is defined as the "beliefs, values, and customs and material traits of a religious, social or racial group" [56]. The latest trend in online services is to offer personalisation of the service in such a way so as to suit and accommodate the needs of the user. AMSs therefore need to introduce this element into their services so that a greater range of users are able, and inclined, to utilise the service; this can be achieved through various different means, such as, for example, language options, display settings, customised pages, etc. Importantly, every culture has different views and opinions owing, and so developing trust is a very important role [28].

G. *Disabilities (D):*

Disabilities are defined as "impairments that might hinder someone's routine activities" [26]. Nowadays, many different types of users are found on the internet; this might even include people with disabilities, such as visual impairment, blindness, deafness, etc.

H. *Assistive Technologies (AT):*

Assistive technology is defined as "a technology that might facilitate the operation of a computer or some other technology" [54]. This factor will evaluate whether or not the access management system offers any degree of compatibility with Assistive technologies.

IV. Evaluation of FAMS

Table 1. summarises a critical review of an extensive evaluation of existing FAMS with various different criterias. A tick (✔) means that there is strong evidences which show FAMS offer these criteria according to specific references; however, a cross (✖) means there is no any evidence to suggest that these systems offer the required criteria, and a question (**?**) means that there is no information about these criteria.

TABLE 1. EVALUATION OF CURRENT FEDERATED ACCESS MANAGEMENT SYSTEMS

FAMS	General criteria for FAMS					Accessibility and Usability					
	T	S	P	N	I	D	L	C	AT	U	A
OpenID	✗ [11]	✗ [11]	✗ [12]	✓ [12]	✗ [21]	✗ [13]	✓ [9]	?	?	✗ [11]	✗ [11]
Shibboleth	✓ [14]	✓ [11]	✓ [14]	✓ [22]	✗ [21]	✗ [15]	?	?	?	✗ [11]	✗ [11]
OAuth	✗ [16]	✓ [11]	✓ [16]	✓ [16]	✓ [16]	✓ [18]	✓ [17]	?	?	✓ [11]	✗ [11]
Liberty Alliance	✓ [23]	✗ [11]	✓ [23]	✓ [23]	✓ [23]	✗ [24]	?	?	?	✓ [11]	✗ [11]
Microsoft Passport	✗ [19]	✗ [11]	✗ [19]	✓ [19]	✗ [20]	✓ [19]	✓ [20], [19]	?	✓ [19]	✓ [11]	✓ [11]
FingerID	✗ [25], [30]	✓ [11], [30]	✗ [11, [30]	✗ [25], [30]	✓ [11], [30]	✗ [25], [30]	?	?	?	✓ [11], [30]	✓ [11, [30]

A more detailed critical and extensive review and evaluation of existing FAMS with different criteria will be presented in the conference. Following the analysis of the existing access management systems, the need for an efficient federated access management system was considered which would do justice to its name. Therefore, a new system has been proposed with the addition of a new term to the existing name: Ubiquitous Access Management System(UbAMS)[29].

V. CONCLUSION

There are various solutions for the issues raised in this paper. One possible approach of AMSs is to follow a ubiquitous approach which may perform on multiple systems. The differentiating aspect regarding the ubiquitous systems approach could be that the decision-making power of the system should not be embedded within it; rather, it should be according to a standard policy to be followed by all the access management systems. The standards might induce uniformity across the systems, as well as produce effective changes whenever there are any required modifications [2], [29].

UbAMS might ultimately enhance the performance of FAMSs and perform the effectiveness expected from federated access management systems. This system could enable users to access their accounts from any system i.e. one log-in identity may be sufficient to gain access to all the federated access management systems. It might prove to be a revolutionary development since existing systems do not currently offer this type of unified service. This system not only offers a single sign-in on all FAMS, but could also cater to all different needs of users, such as needs to personalise the service with respect to language, culture or disabilities, etc [29].

REFERENCES

[1] H. C. Choi1, Y. H. Yi, J. H. Seo, B. N. Noh, H. H. Lee, "A Privacy Protection Model in ID Management Using Access Control", *Lecture Notes In Computer Science*, vol. 3481, pp. 82 – 91, 2005.

[2] R. Wilhelm, M. Maffei, "Ubiquitous Verification of Ubiquitous Systems", *Lecture Notes in Computer Science*, vol. 4239, pp. 73 – 81, 2006.

[3] A. Squicciarini, A. Bhargav, A. Czeskis, E. Bertino, "Traceable and Automatic Compliance of Privacy Policies in Federated Digital Identity Management", *6th Workshop on Privacy Enhancing Technologies*, 2006

[4] CafeSoft, "Access Management", 2010.

[5] F. Pimenta, C. Teixeira, J. Pinto, "GlobaliD: Federated identity provider associated with national citizen's card", I*nformation Systems and Technologies (CISTI), 2010 5th Iberian Conference*, Spain, *IEEE*, 2010.

[6] A.John, "Future of identity management is…now!" *Identity and Access management*,2010.

[7] J. Noel Colin, T. D. Le, D. Massart, "A Federated Authorization Service for Bridging Learning Object Distribution Models", *Lecture Notes in Computer Science*, vol. 5686, pp. 116–125, 2009

[8] R. Akbani, T. Korkmaz, and G.V.S. Raju, "A Hybrid Trust Management System for automated Fine-Grained Access Control*", IEEE*, 2009

[9] B. Ferg et al., *"OpenID Authentication 2.0—Final", OpenID Community*, Dec. 2007.

[10] Shibboleth, "shibboleth Web Single Sign-On and Federating Software",.*internet2.edu*, 2010.

[11] S. Alotaibi, D. Argles, "FingerID: A New Security Model Based on Fingerprint Recognition for Distributed Systems", *IEEE*. pp. 284-289, February 21-23.

[12] E. Prodromou, "OpenID Privacy Concerns", 2007.

[13] J. Zhou, "OpenID usability is not an oxymoron", *FactoryCity*, 2008.

[14] Oxford Computer Group , "Achieving Interoperability between Active Directory Federation Services and Shibboleth", 2007.

[15] R. L. Morgan, S. Cantor, S. Carmody, W. Hoehn, K. Klingenstein, "Federated Security: The Shibboleth Approach", *Educause Quarterly*, Vol 27, No. 4, 2004.

[16] M. Simhachalam, "Securing REST Web Services With OAuth", *Oracle Corporation*, 2009

[17] G. F. Fletcher, "OAuth Extension for Specifying User Language Preference - Draft 2", 2007.

[18] W3C, "Accessibility issues of social Web", *W3C*, 2010.

[19] N. Shah, R. Ye, "Understanding Microsoft Passport", MSc Thesis, North Eastern University.

[20] D. Berlind, "Microsoft's Identity Chief: After Passport, Microsoft is rethinking identity", 2005.

[21] D. Chadwick, S. Otenko, W. Xu, "Adding Distributed Trust Management to Shibboleth", University of Kent.

[22] L. Ngo, A. Apon, "Using Shibboleth for Authorization and Authentication to the Subversion Version Control Repository System", 2007.

[23] The Free Library, "Liberty Alliance Builds Global Trust Framework for Identity Federations Spanning Industries and Regions", 2007.

[24] P. Judge, S. Shankland "Liberty - is usability compatible with security?", *ZDnet US*, 2002.

[25] S. Alotaibi, D. Argles, "FingerID: A New Security Model Based on Fingerprint Recognition for Personal Learning Environments (PLEs)". In: *IEEE Engineering Education, IEEE* . pp. 142-151, 2011.

[26] Houghton Mifflin Harcourt, "American Heritage Dictionary, Dictionary of the English Language, Fourth Edition", 2010.

[27] S. Melissa, "Introduction to the Federated Access Management in the UK", JISC, 2009.

[28] P. B. Lowry, D. Zhang, L. Zhou, X. Fu, "The Impact of National Culture and Social Presence on Trust and Communication Quality within Collaborative Groups", *Proceedings of the 40th Hawaii International Conference on System Sciences*, 2007.

[29] S. Alotaibi, M. Wald, D. Argles, "From Access Management System (AMS) to a Ubiquitous Access Management System (UbAMS), over Federated Access Management System (FAMS)", *IEEE*, June 2011.

[30] S. Alotaibi , M. Wald, D. Argles,"Using Fingerprint Recognition in a New Security Model for Accessing Distributed Systems". *the International Journal of Intelligent Computing Research (IJICR)*, 2 (1). pp. 491-500. ISSN 2042 4655.