Mangiuc, Dragos Marian

Article

Cloud Identity and Access Management – A Model Proposal

Journal of Accounting and Management Information Systems (JAMIS)

Provided in Cooperation with:
The Bucharest University of Economic Studies

Suggested Citation: Mangiuc, Dragos Marian (2012) : Cloud Identity and Access Management – A Model Proposal, Journal of Accounting and Management Information Systems (JAMIS), ISSN 2559-6004, Bucharest University of Economic Studies, Bucharest, Vol. 11, Iss. 3, pp. 484-500

Accounting and Management Information Systems
Vol. 11, No. 3, pp. 484–500, 2012

CLOUD IDENTITY AND ACCESS MANAGEMENT – A MODEL PROPOSAL

Dragoş Marian MANGIUC[1]
The Bucharest University of Economic Studies, Romania

ABSTRACT

Even if in a typical organization, where applications are deployed within the organization's perimeter, the "trust boundary" is mostly static and is monitored and controlled by the IT department; with the adoption of cloud services, the organization's trust boundary will become dynamic and will move beyond the control of IT. With cloud computing, the network, system, and application boundary of an organization will extend into the service provider domain. This loss of control continues to challenge the established trusted governance and control model, and, if not managed properly, will obstruct cloud service adoption within an organization. Based on both literature review and action research, the paper at hand is a synthesis for the results of a thorough review of the opinions and study attempts performed during the last years among Romanian and foreign companies, in order to find and formulate a consistent model for the integrated identity and access management, and, if possible, a cloud extension of the model. The paper is a part of a larger research performed by the author in the field of cloud computing and the neighboring technologies.

Cloud computing, Identity as a Service, Identity management, Access management, Control systems

INTRODUCTION

Traditionally, software applications within an organization's information system are deployed and placed inside the organization's boundaries. Thus, the organization has a "trust area", which is defined by static methods, being monitored and controlled by the experts of the IT department. In most cases, the "trust area" encapsulates the core organizational network, systems and applications that are managed in-house, being organized in the form of a data center. The data center

[1] *Correspondence address*: Faculty of Accounting and Management Information Systems, Bucharest University of Economic Studies, 6, Piata Romana, Romania; Email: mangiuc@gmail.com

can be either managed by experts from within the organization, or outsourced to an external service provider (in this case, the organization usually reserves the right to control and to have the final word on the manner security policies are formulated and implemented). In a "traditional" model, the access to the information resources of the organization is secured through a set of specialized systems, implemented at the network level.
This category usually includes:

- Tunneling and virtual private networks (VPN);
- Intrusion detection systems (IDS);
- Intrusion prevention systems (IPS).

However, the referred model is not able to provide a reasonable level of security if the organization chooses to implement its information system based on cloud components. In terms of security, the main consequence of a "migration" to the cloud is the expansion of the "trust area" beyond the current scope of the IT department's control. The traditional components of the organization's information system (network, system, applications) will expand in an area belonging to the cloud-based service provider (especially if e-commerce, outsourcing or collaboration in the virtual environment have a significant weight in the organization activity). This loss of control tendency usually requires reconsidering the governance and control model of the organization and, if not properly managed, can significantly affect the success of a migration to the cloud.

1. RESEARCH METHODOLOGY

This paper is one of the results of a larger research performed by the author in the field of cloud computing and *Enterprise 2.0* technologies, and also continues a previous doctoral research in the field of computer-assisted audit tools and techniques, whose final results were publicly defended in order to be validated by both the scientific and academic community. The main goal of the aforementioned research was the identification of some new areas of applicability for the modern knowledge-based information technologies in the field of computer-based audit.

Wherever possible, a direct identification of the practitioners' expectations was attempted by means of direct interviews and also by means of an empirical study questionnaire. The questions for the empirical study were carefully designed so as to get unbiased, objective answers. The members of the target group were encouraged to add their own observations regarding the questionnaire. Validation of the research conclusions was performed by means of an informal discussion with some "real life practitioners", members of some companies which performed or are in the process of performing a migration to cloud-based services. Also, professionals from a cloud migration assistance and consulting company were interviewed.

In case some other author's opinion was enclosed in the paper, whether in exact quotation or synthetic form, a complete mention of the source identification information was made. Some of the data in the paper is based on the results of some previous scientific or market research studies that were credited accordingly.

The author has over ten years of previous experience in the research area, and also a series of previous research results (published articles, conference attendances and doctoral research). By defending the research results at the proceedings of such a prominent scientific conference, attended by both scholars and practitioners bearing some interest in the research area, the author attempts to get further validation of his opinions, both confirmation and rejection of the aforementioned opinions' scientific and practical importance being welcome.

2. THE IDENTITY ACCESS MANAGEMENT (IAM) SOLUTION

By contrast to the traditional approaches, which are basically monolithic, and whose formulation and implementation require a massive adaptation effort for the organization, *Identity Access Management* (or *IAM*) is a new way of thinking the organizational security systems that may represent a viable alternative, having in the same time the advantage of an accelerated implementation. The most common security architecture nowadays includes several distinct levels, each one having its own services and processes. This approach has at its core a directory service (such as *LDAP* or *Active Directory*) that contains and stores security attributes for the users in the area of the organization. In the case of a large organization, the landscape can be even more complicated, with several parallel distinct directory services, maintained for the used operating systems compatibility reasons, as *Active Directory*, for example, runs only under Windows, while *LDAP* does not support the operating systems produced by Microsoft. Another source of complexity derives from the need to "melt together" more or less compatible security systems, in the case of mergers or acquisitions driven by the economic environment.

An analysis performed by the author in the field of regulations and applicable conceptual frameworks for the organizing of the IAM, reveals the existence of the following core processes:

- **User management** – identity lifecycle management activities, for each user of the organization;
- **Authentication management** – the effective and error-free management of the user identity genuineness determination process (the ability to determine whether he or she is who claims to be);
- **Authorization management** – the ability to determine without any error the resources that each user is entitled to access, as well as the user's rights in relation to the accessed resources;

- **Access management** – the implementation of access control policies, so as to be able to provide the correct answer to an access request concerning a resource from within the organization;
- **Management and dissemination of access data** – a set of processes which ensure the transmission of the identity and access data between the information components of the organization;
- **Audit and operational monitoring** – compliance monitoring, auditing and reporting processes, for the compliance of the users' access with the effective access security policies defined for the organization.

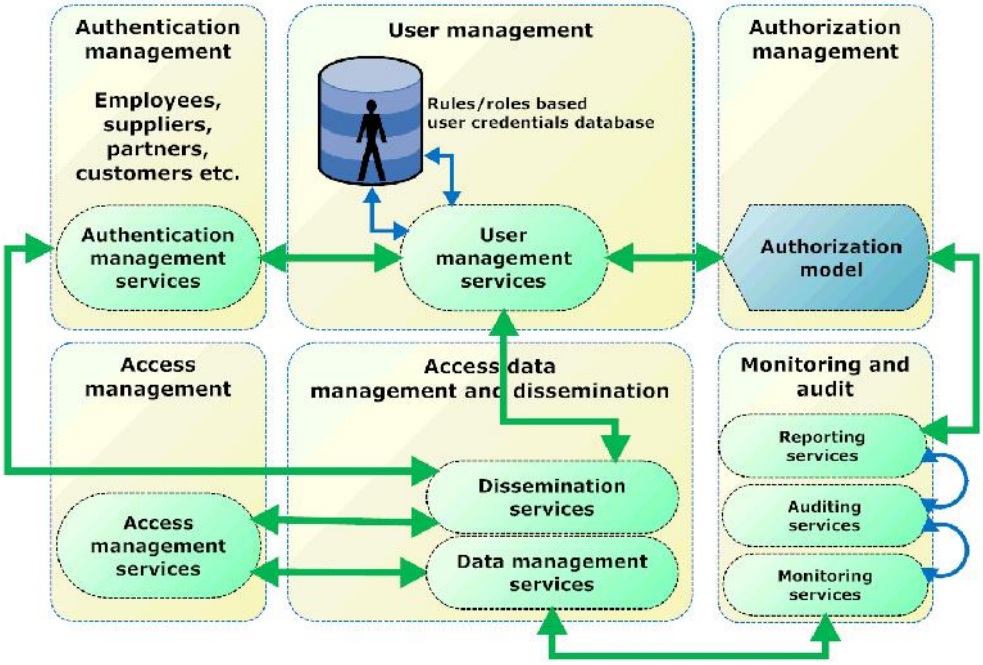
Based on these "core" processes, a coherent functional type architecture may be proposed, as depicted in Figure 1.

Moreover, IAM should allow, at the operational level, the following activities to be performed:

- **Attributes management** – an activity that involves the management of the user rights package lifecycle (creation, revocation, update etc.) and aims to minimize the risk of inappropriate use of the user accounts and eliminate any attempts to abuse access. Also, the scope of this activity covers the password management operations, along with password testing for vulnerabilities identification (in case of various types of attacks).
- **Authorization policies management** – involves activation and deactivation for the privileges needed by users, in order to access different resources belonging to the organization. A proper management of the authorization policies implies that each user is assigned only those privileges that coincide with his or her status within the organization. The activity may also be used to enhance the security of Web services, Web applications, legacy applications that are still used, documents, files and biometric security systems.
- **External identities management** – involves the management of trust relationships established between different organizations. It is a common situation that a group of organizations share information about the users and the resources held, in order to enable collaboration and transaction-based data exchange.
- **Compliance management** – involves the monitoring and tracking of the access rights and privileges, in order to provide security for the organization's resources. In addition, the activity allows auditors to assess compliance with the various control access internal policies, and also compliance with the "best practices" standards, such as the segregation of duties, access monitoring, systematic auditing and reporting. For example, the authentication process must be designed so as to allow auditors to certify that only authorized users have access to confidential business data.
- **Authentication and authorization centralization** – a centralized authentication and authorization system eliminates the need to implement these functions at the level of each application. Moreover, it allows the

development of some "general level" applications, which have total transparency to the security system.

Figure 1. **IAM functional architecture schema**



These activities are cyclical and are essentially depicted in Figure 2.

According to the author, the aforementioned model can be also extended for the case of organizations that outsource a part of their management information system (or even the entire information system), migrating their own applications to cloud-based versions. Organizations which have already significantly invested in identity management systems and policies might adapt their existing infrastructure to the new context. Those who have not yet made such investments have an additional option, the appeal to a range of providers of such services in the cloud. As standardization in the field of IAM is not mature at present, and there are multiple parallel standards, achieving various stages of completion, it is very likely that the multiprotocol services offered by some suppliers to be a valid option in the long term (Everett, 2011). Such services are usually offering portals that can be used to harmonize the security policies for the various organizations having interconnected systems and to expand internal security policies within the organization to the cloud.

Figure 2. **IAM core operational activities**

3. IDENTITY ACCESS MANAGEMENT – THE FRAMEWORK

In addition to the identification of the requirements, advantages and drawbacks of standard IAM principles implementation, it is of main importance to perform an analysis of the main attempts to standardize the field, as they may prove crucial to the success of its adoption. The analysis of the relevant literature reveals that there are a few major standards in IAM:

Security Assertion Markup Language (*SAML*) – is the most advanced, comprehensive and popular standard for the authentication (login) process of the users of cloud-based services. Once the user logs into the identity management service, he or she can freely access all the applications and cloud services that are included in the identity management service's trust area (Sivan, 2003). Where necessary, the SAML standard allows strong authentication, as well as multiple (dual-factor or multifactor) authentications. The techniques chosen for the multiple authentication process depend directly on the hazards that are intended to be minimized, and, according to some authors, may serve to reduce the effectiveness of *phishing* attacks very frequent in the Internet environment (Rosencrance, 2002). Besides, multifactor authentication can be an element of defense in the case of "man-in-the-middle" attacks, when a user in good faith may become a victim of a trojan or an automated attack system (attack bot). Using the SAML standard, which allows delegation of the authentication model to a third party, a cloud-based service provider can delegate the authentication policies to the organization having

the status of customer, allowing the cloud service provider to be independent in relation to the authentication requirements of its customers (Harding, 2005).

Service Provisioning Markup Language (*SPML*) – a conceptual framework developed (by the *Organization for the Advancement of Structured Information Standards – OASIS*) as an XML application that enables organizations engaged in cooperative relationships to exchange free information about their users, services and resources (Sodhi, 2004). SPML is an emerging standard that can enable organizations to automate the preparation of user identities to be used in the cloud. For example, an application running in the cloud may request the organization's ERP system (which also runs in the cloud) the update of the information on user accounts. To the extent that they assure SPML support, all Software-as-a-Service (*SaaS*) vendors will be able to create accounts in real time for the new users, and this grants them increased efficiency when compared to the classic, pre-registered users-based management system. In this modern version, the cloud-based service provider extracts from a SAML sequence the attributes of a new user, creates a real-time SPML message, and sends it to an authentication service that adds the new identity in the cloud-based users database. SPML adoption may lead to standardization and automation of the access and rights management for cloud services without chaining customers to a proprietary format.

eXensible Access Control Markup Language (*XACML*) – a second standard developed by OASIS and also XML-based, the XACML language is basically an access control language, made for the security policies and access decisions management (Mazzoleni *et al.*, 2008). From a technical standpoint, the standard provides an XML schema for a general security policies definition language, which can be used to protect any type of resource, and also to fundament decisions regarding the access to the resources. The XACML standard is not limited to providing a model for a policy definition and maintenance language, but also contains a proposal for a policies management and access requests solving environment. In addition, the standard specifies a request-response type protocol, which the application environment may use to communicate with the point where the decision is made. Both the access request and the response to it are specified by using XML. Most of the applications' (whether they are "traditional" or Web-based applications) authorization system include specialized modules that allow or prohibit access to certain functions or application resources based on the rights initially assigned to the user. By contrast, in an IAM-based centralized architecture, the application-specific authorization models render quite difficult to simultaneously define access rights for a user over all the applications. Therefore, the goal of XACML is to provide a unified language, a method of access control and a way to enforce the implementation of common security policies across all applications that share the same standard of authorization. Authorization decisions are based on a large number of policies and rules about a user's position and

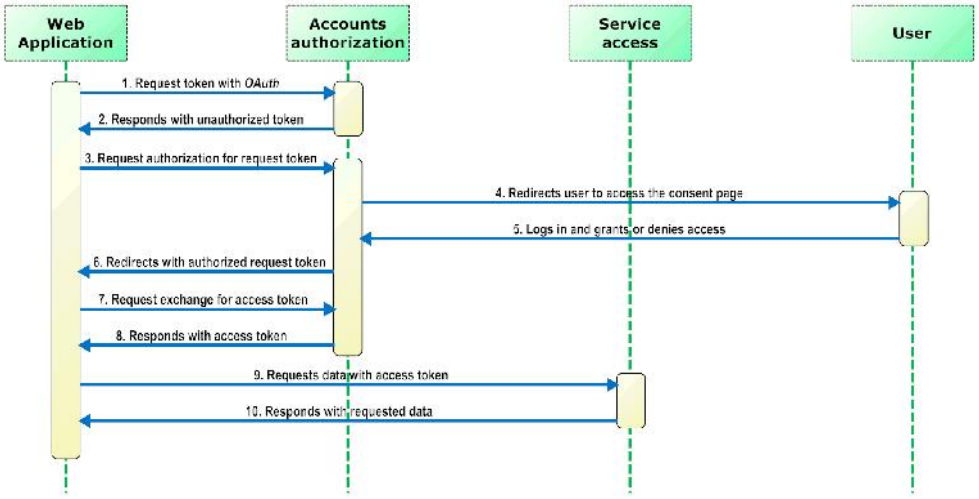
function. To conclude, XACML allows unified authorization policies for multiple services.

Open Authentication (*OAuth*) – an emerging authentication standard that allows users to share their resources (from images and documents, to contact lists and bank accounts) stored by a cloud-based service provider to another cloud-based service provider, without the need to send the actual authentication information (username and password). OAuth is an open protocol, designed to allow the authorization between different providers of cloud-based services through an application programming interface (API) – which provides a simple and standardized working method, usable by both the "traditional" and the next-generation mobile systems (Android, IOS, etc.). In terms of a programmer or an applications developer, OAuth can be perceived as a way to interact with protected or confidential datasets. In terms of a cloud-based service provider, it may be perceived as a standard method to access your own data hosted by another provider, without disclosing your login details. According to the author, OAuth may also be used at an organization or business level, in order to design and implement a system of "unique identification" (usually known as a *Single Sign On – SSO* system). Single sign-on (or *SSO*) is a mechanism whereby a single action of user authentication and authorization can permit a user to access all computers and systems where he or she has access permission, without the need to enter multiple passwords (Bruno-Britz, 2009). Single sign-on reduces human error, a major component of systems failure and is therefore highly desirable, but difficult to implement. OAuth facilitates, by its own structure, the mutual authorization of two Web services which need to interact, without them being strongly connected in a common architecture (Connolly, 2010). Like *OpenID*, OAuth is rooted in a client-oriented approach, and is designed to allow the customers to access their data sets hosted by multiple vendors. A few months ago, Google announced the development of a hybrid standard, compatible with both OpenID and OAuth (Schwartz, 2010), which would have the advantage of simplifying the authorization process. The most common scenario for the use of the OAuth standard is depicted in Figure 3 by means of an UML sequence diagram describing the use case.

OpenID – represents an open and decentralized standard for user authentication and access control, which allows a person or application to identify to more than one Web service with the same digital identity. Its mode of operation includes the replacement of the "traditional" authentication process (with user name and password), allowing a user to authenticate once in order to gain access to multiple applications and systems. OpenID is focused on services provided to the end users (Google, eBay, Yahoo, etc.). The adoption of the standard by organizations is still very weak, because there are still serious doubts about the provided level of security; some authors argue that this protocol may favor *phishing* attacks that compromise a user's identity (Weiskotten, 2008).

Information cards – is another open standard for the identity management on the Web. Its development is managed by the *Information Cards Foundation* (which includes among its members representatives of Google, Microsoft, PayPal and Oracle). As its authors state, the purpose of the standard is "to reduce identity theft through securing identity in the digital environment, without recourse to the classical method of introducing a username and password" (Anderson *et al.*, 2008). Users may use an information card to state their digital identities on different sites without the risk of compromising their login ad authentication data. Notice that this standard's purpose is almost identical to that of OpenID. But unlike OpenID, which is intended primarily for home users in relation to the entertainment applications, information cards is meant for critical scenarios (such as banking transactions), where resistance to *phishing* and support for authentication mechanisms (such as *smartcards*) are a must. Information cards (also known as *I–Cards*) may be issued or accepted by any cloud-based service provider. Some authors consider that although this system provides a high level of protection against *phishing* and identity theft, it suffers, however, from a number of shortcomings, which prevent it from becoming a widespread industry standard (Button, 2010). The most important of these shortcomings is that the Web site or application that the user attempts to authenticate on with an information card must have explicit support for Information Cards, in other words, must be affiliated to the foundation that is developing the standard; otherwise the attempt will be useless. As Information Cards Foundation is getting new members, the system increases its scope and usefulness, but now is considered to have limited use. Currently, a user of Microsoft Windows Live ID (a service issuing information cards) can use an *I-Card* to authenticate in other Web applications such as Microsoft's MSDN or TechNet.

Figure 3. ***OAuth*** **employment scenario**



Open Authentication (*OATH*) – the direct competitor of OAuth, the other standard having the same name, but different acronym, OATH is a joint effort of some large companies in the computer industry to build an architecture that allows "strong" (industrial level) authentication for any user and any electronic device in any type of network. The purpose of this application is to ensure the unification of the three main methods of authentication that are now industry standards:

- Authentication based on SIM (*Subscriber Identity Module*) in the GSM or GPRS networks;
- Authentication using the public key infrastructure (*Public Key Infrastructure – PKI*);
- Single use password authentication based on an electronic token (*One Time Password – OTP*);

This protocol aims to increase the safety degree and the level acceptance of the three methods mentioned above, so as to be used in the cloud environment, and to become compatible with each other.

Open Authentication API (*OpenAuth*) – is an application programming interface (API) created by America Online (*AOL*) that allows some sites and applications to authenticate to AOL and the AOL Messenger. In this way, an AOL-registered user may have instant access to third-party applications built on the AOL platform and employing the AOL-based services. According to a recent study of OpenAuth (Rosini, 2010), its main advantages are:

- A secure method of registration; as user registration data are never sent to the sites or applications that the user gets access to;
- A safe way to control which sites have the right to read private or protected data elements;
- Automatic granting of permissions and rights; but only if the user consents to the procedure;
- Request user agreement when attempting to read any private or protected data element;
- Direct access to any other OpenAuth compatible site, no longer requires additional authentication.

This protocol is proprietary in nature (because AOL owns all rights to it), so it cannot be adopted in its current form by the community of cloud-based service providers.

As a result of the review of the aforementioned standards and protocols specifications, the author performed a comparative analysis of the specifications, trying to summarize them from two main perspectives: the requests concerning the cloud-based service provider, and the requests concerning the potential beneficiaries of its services. The results are presented in Table 1.

Table 1. ***IAM*** **standards face-to-face**

Standard or protocol name	Supporting companies	Open standard	Cloud provider requests	Cloud beneficiary requests
SAML	Oracle, IBM, Novell, Computer Associates, Microsoft, Sympified, TriCipher, Ping Identity	YES	Allow customers to delegate authentication and choose authentication methods that enable adoption of the cloud service.	Strong authentications, Web-based SSO, avoid identity duplication; protect privacy by sharing attributes only by consent.
XACML	Oracle, Computer Associates, Jericho Systems, IBM, CISCO, Securent, Red Hat	YES	Allow authorization that may represent complex policies, required by enterprise-scale applications and administrators.	A standardized mean to formulate authorization policies across a large set of cloud services and separate authorization and enforcement procedures from the application.
OAuth	Google, Twitter, Facebook, Plaxo	YES	Allow users to access their data (hosted by another service provider) while protecting their account and credentials information, which is not sent.	Publish and interact with protected data stored by one provider and accessed by another provider using a standard API and without disclosing credentials.
OpenID	Google, IBM, Microsoft, yahoo, Orange, payPal, VeriSign, AOL, Yandex, UStream	YES	Provides SSO for consumers participating in this federated identity service.	Adoption avoided due to some trust issues.
OATH	VeriSign, SanDisk, Gemalto, Entrust	YES	Unification across three widely used industrial standards.	Unification across three widely used industrial standards.
OpenAuth	AOL and partners	NO	Support AOL users access to third party applications using AOL or AIM user IDs.	Support for single authentication across multiple applications (by AOL partners only).

4. IDENTITY ACCESS MANAGEMENT AND THE CLOUD

When compared with their intra-organizational counterparts, the methods of access and identity management used directly in the cloud are still in an early development stage. As shown in a previous paper by the same author (Mangiuc, 2011), the standards of security management in the cloud are extremely diverse, differing significantly from one provider to another, regardless of the provided cloud computing component (software, platform or infrastructure). An analysis attempt, that the author performed by comparing the offers of the main cloud services providers, reveals the existence of different degrees of maturity in the field of identity and authentication management, as summarized in Table 2.

Table 2. **Cloud-based *IAM* maturity levels**

DOMAIN	SAAS	PAAS	IAAS
User Management, New Users	Capable	Immature	Aware
User Management, User Modifications	Capable	Immature	Immature
Authentication Management	Capable	Aware	Capable
Authorization Management	Aware	Immature	Immature

The above results have been formulated taking into account the dynamic nature of the users, systems and applications which require IAM in the cloud, and also the way they address the four main domains of the automatic identity and authentication management process. The comprehensive explanation and meaning of each judgment in the above table is explained in detail in Table 3.

The reference data presented in Table 3 allows a comparison between the description of the different maturity levels taken as a standard (in Table 3), and the actual maturity level of the IAM services; examined through the activities and processes previously defined in the model. Thus, the subsequent analyzes will be able to focus differently on each area, depending on the reached maturity level.

Table 3. ***IAM*** **maturity levels criteria**

DOMAIN	IMMATURE	AWARE	CAPABLE	MATURE	INDUSTRY ST.
User Management, New Users	Manual, no formal process.	Manual, with formal process.	Automated when possible, several processes.	Automated, multiple processes.	Automated, single standardized process.
User Management, User Modifications	Manual, per application.	Manual, by application group.	Manual or automated (for an application group).	Automated, by application and resource type.	Automated across applications.

Authentication Management	Manual, no common security policy.	Per application, no common authorization mechanism.	Common authentication mechanism, no common authentication module.	Common authentication module, minimal credentials, common security policy.	Standardized authentication mechanism as a component service to applications, standard security policy
Authorization Management	Manual, no rule-based authorization, no role-based authorization.	Per application, no common authorization mechanism.	Common service, no common module.	Common module, application-specific attributes, separately maintained	Standardized mechanism, centrally managed attributes, support role, rule-based

Although all the previously mentioned components belonging to the organization-level specific IAM implementation practices and processes are fully applicable to the cloud-based services, the identified, cloud-level specific, IAM functions are:

- **Identity management in the cloud** – these functions should focus on the cloud users identity lifecycle management (create, delete, federate, password and rights management, etc.). Organizations that are unable or unwilling to participate to a federated identity management architecture are free to turn to the cloud-based identity management services (*Identity-as-a-Service*), (Kearns, 2008). This kind of service handles the synchronization of the company's internal directories with its own directory (which usually includes data from many organizations) and acts as an identity "proxy" type provider for each subscribing organization. Regardless of the alternative chosen by an organization, the result is the avoidance of duplication for the set of identity and identification attributes; as well as their storage in the cloud. However, because of the different and relatively incoherent manner cloud-based service providers apply the existing standards (which are not all at a satisfying maturity level), the organization acting as customer may be required to use completely different methods of communication with each of its suppliers. A recent review of the area (Cerf, 2011) reveals important shortcomings, such as the manual processes, the externally delegated administration, the transmission of sensitive data by means of unprotected spreadsheets, the execution of proprietary scripts, both for the customer and the supplier. According to the author, a model having such issues cannot be manageable on the long term, the implementation of standards being therefore mandatory.
- **The Single Sign-On (*SSO*) and federated identity implementation possibility assurance** – organizations that intend to implement these mechanisms are usually able to choose between two major types of

architecture. The first option is the traditional one, the implementation of an identity services provider within the organization; while the second involves integration with the services of a cloud-based identity provider. As both alternatives have their own advantages and disadvantages, as noted in a previous paper by the same author (Mangiuc, 2011), one cannot finally and absolutely decide in favor of one of them. A comparison of the two approaches is presented in Table 4.

Table 4. ***IAM*** **approaches comparison**

	Organization-based identity services provider	**Cloud-based identity services provider**
Strong points	• Consistent with internal policies, processes and access management • Direct access to the service-level agreement and the identity provider's security level • Incremental investment in the existing identity architecture in order to assure federation in the future	• Some cloud identity management use cases are migrated to the cloud-based services provider, hiding the complexity of some standards (or versions of the standards) • Only small architectural changes are needed • Once the synchronization is complete, users can sign to cloud applications using corporate credentials and authentication policies
Weak points	• In the absence of federation, the addition of the identity life cycle management for non-employees may lead to serious inefficiencies	• Lack of details visibility, as the company relies on a third party • Overall performance depends solely on the performance level of the cloud service provider, not fully visible for the beneficiary • The lack of detailed reports for compliance reporting • Non-uniform attribute definition may render the process very complex (complex synchronization)

- **Authorization management** – medium to large organizations have, in most cases, specific requirements for the authorization of their users in the cloud-based services (such as the assignment of employees' rights based on their position in the company). In some cases, an application may require role-based access control (RBAC), and the cloud-based authorization system may be insufficiently developed to provide security at this level of detail. The direct consequence is that the services provided through the cloud won't respond to the requirements established within the organization. Most cloud-based services provide two basic roles: administrator and user. In such circumstances, it is a common practice that the role of administrator has, among other things, full privileges in the user authentication and security policies statement areas, including the cases

when the real situation requires a more nuanced approach. A recent study shows that XACML is now the preferred standard for the formulation and implementation of authorization and authentication policies (Kearns, 2011). The author's research on the other hand, revealed that currently there is no cloud-based service able to provide support for XACML, and this situation may cause serious issues when migrating security policies and user rights from within the organization to the cloud.

- **Compliance management** – the architecture and the set of practices associated with access and identity management in the cloud (IAM) have an essential role in the overall assessment of the effectiveness of the business processes with IT support in an organization; and therefore they are of major importance in providing and managing compliance. The well implemented IAM practices and processes are able to massively improve the effectiveness of the controls enforced by the conceptual framework applied in order to ensure compliance. For example, through the full automation of the access rights granting and withdrawal process, organizations will be able to reduce the risk of unauthorized access. Practices and processes within the IAM provide a centralized perspective over the business operations, and also an automatic processing element that can stop the outside attacks before they occur. However, given the low and superficial level of current adoption of the SAML, SPML and XACML standards by the cloud service providers, the compliance of each provider should be evaluated separately, based on parametric processes, depending on the specific case analyzed.

DISCUSSION AND CONCLUSIONS

According to the author, access and identity management remains one of the main factors holding back the adoption of cloud based services and technologies. The needs of an organization in the field of the IAM range from the global security of the cooperation with the partners; to the global security of the access for the employees who may require sensitive, private or secret information from anywhere and at any time. Although, technologically speaking, the basic components are in place, the migration and adaptation of these technologies, in their current form, to the cloud-based services level will not lead directly to the expected achievements of efficiency, effectiveness and business agility. The overwhelming volume of dynamic processing resources available in the cloud, along with the huge number of users accessing those resources, will provide significant challenges to the scalability and automation of access and identity management. Furthermore, the already existing IAM solutions implemented inside the organization will complicate things. The IAM architecture, in its organizational version, is sufficiently complex and burdened by standards, for its extension to the cloud to become sluggish and costly. This is compounded by the fact that the cloud based

sources of identity information are not always reliable, and also by the fact that the manner cloud-based service providers implement IAM standards is still casual and yet inconsistent with an organization's internal quality standards. Although the SaaS providers are beginning to deliver broad support for standards such as SAML, at the PaaS and IaaS levels, they are almost nonexistent.

The analysis reveals that a small number of cloud-based service providers begin to consider the organization-level requirements in the IAM; including support for the SAML and the SSO technology that facilitates the federated identity management techniques. While almost all these suppliers are very large companies (like Microsoft, Google or Salesforce), facilities offered by the cloud in the field of EAM remain at an elementary level (Kobielus, 2002). According to the author, only the pressure from the beneficiaries of cloud services will accelerate the adoption of core standards as SAML, SPML, XACML, along with an API-type interface that supports the automation access and the identity management processes.

The need for confidence in the cloud services provider and the need to unconditionally handle the own data to be managed externally are other impediments (both technical and psychological), as organizations do not easily accept to place their identity management data sources outside their borders. The issue is aggravated by the fact that many usage scenarios require the duplication of the data sets or the storage copy of the customer organization’s data sets in the cloud. The synchronization of multiple identity and access management services remains a challenge, even for the very large organizations, the process being facilitated (perhaps) in the future by the adoption of common standards. According to the author, in order to avoid unpleasant and costly surprises, any organization migrating to the cloud must include the IAM strategy as a part of its general plan to adapt to the new paradigm. It is considered that the most important factor for the success of IAM in the cloud is the existence of a coherent and articulated directory, as well as the existence of identity management capabilities within the organization (architecture, systems, user life cycle management processes, audit and compliance procedures). They are traditionally stored in a private or public cloud, depending on the option of the organization.

To sum up, it is considered that any organization intending to use cloud-based services (IaaS, PaaS, or SaaS) should formulate and consider its own operational requirements, security-related requirements, and also the requirements related to the protection of private information and compliance, the support level that suppliers provide for the IAM practices and standards, along with the present and future needs related to the lifecycle management of each user. It is usually considered that organizations that have serious deficiencies in their own IAM's, should take advantage from the Identity-as-a-Service offers when they need to

interface with many partners; or intend to participate in numerous federated identity schemes. To avoid later and hard-to-bear costs, organizations must prepare their own IAM strategy and up to date architecture, and then try to extend them to the cloud, by using standard protocols like SAML, SPML, XACML, to the maximum extent these standards compatibility support is offered by the providers of the cloud services.

REFERENCES

Anderson, K.B., Durbin, E. & Salinger, M.A. (2008) "Identity Theft", *The Journal of Economic Perspectives*, vol. 22, no. 2:171-192

Bruno-Britz, M. (2009) "Streamlining Single Sign-On", *Bank Systems & Technology*, vol. 46, no. 4: 39-46

Button, K. (2010) "Phishing Tackle", *Bank Technology News*, vol. 23, no. 10:1-9

Cerf, V.G. (2011) "Secure identities", *IEEE Internet Computing*, vol. 15, no. 4: 96-98

Connolly, P.J. (2010) "OAuth is the 'Hottest Thing' in Identity Management", *eWeek*, vol. 27, no. 9: 12-14

Everett, C. (2011) "Identity and Access Management: the Second Wave", *Computer Fraud & Security*, vol. 2011, no. 5:11-13

Harding, P. (2005) "SAML 2.0 simplifies federation", *Network World*, vol. 22, no. 48: 40-40

Kearns, D. (2011) "XACML-Based Directory Server", *Network World*, vol. 4, no. 8: 60-71

Kearns, D. (2008) "The 'identity as a service' controversy: * Using the phrase 'identity as a service (IaaS)' legally", *Network World*, vol. 1, no. 7:16-19

Kobielus, J. (2002) "Microsoft Supports SAML, Sort Of", *Network World*, vol. 19, no. 32: 39-45

Mangiuc, D.M. (2011) "Enterprise 2.0 – Is the Market Ready?", *Journal of Accounting and Management Information Systems*, vol.10, no. 4: 516-534

Mazzoleni, P., Crispo, B., Sivasubramanian, S. & Bertino, E. (2008) "XACML Policy Integration Algorithms", *ACM Transactions on Information and System Security*, vol. 11, no. 1: 29-36

Rosencrance, L. (2002) "SAML Secures Web Services", *Computerworld,* vol. 36, no. 35: 30-30

Rosini, T. (2010) "Newspeople", *Editor & Publisher*, vol. 143, no. 12: 52-53

Schwartz, M.J. (2010) "Google Embraces OAuth Authentication For Apps", *Informationweek*, vol. 6, no. 9: 36-39

Sivan, S.S. (2003) "SAML & Single Sign-On", *Dr. Dobbs Journal*, vol. 28, no. 11:36-45

Sodhi, G. (2004) "User Provisioning With SPML", *Information Security Technical Report*, vol. 9, no. 1:86-96

Weiskotten, J. (2008) "OpenID Single Sign-On", *Dr. Dobb's Journal*, vol. 33, no. 10: 40-45