Complex Adaptive Systems Modeling
a SpringerOpen Journal

RESEARCH Open Access

Cloud identity management security issues & solutions: a taxonomy

Umme Habiba[1*], Rahat Masood[1], Muhammad Awais Shibli[1*] and Muaz A Niazi[2]

*Correspondence:
umme.habiba@seecs.edu.pk;
awais.shibli@seecs.edu.pk
[1]Department of Computing, School of Electrical Engineering & Computer Science, National University of Sciences & Technology (NUST), Sector H-12, Islamabad, Pakistan
Full list of author information is available at the end of the article

Abstract

Purpose: Cloud computing systems represent one of the most complex computing systems currently in existence. Current applications of Cloud involve extensive use of distributed systems with varying degree of connectivity and usage. With a recent focus on large-scale proliferation of Cloud computing, identity management in Cloud based systems is a critical issue for the sustainability of any Cloud-based service. This area has also received considerable attention from the research community as well as the IT industry. Numerous Cloud Identity Management Systems (IDMSs) have been proposed so far; however, most of those systems are neither widely accepted nor considered highly reliable due to their constraints in terms of scope, applicability and security. In order to achieve reliability and effectiveness in IDMs for Cloud, further extensive research needs to be carried out to critically examine Cloud based IDMSs and their level of security.

Methods: In this work, we have holistically analyzed Cloud IDMSs to better understand the general as well as the security aspects of this domain. From the security perspective, we present a comprehensive list of attacks that occur frequently in Cloud based IDMSs. In order to alleviate those attacks, we present a well-organized taxonomy tree covering the most desired features essential for any Cloud-based IDMSs. Additionally, we have specified various mechanisms of realization (such as access control polices, encryption, self-service) against each of the features of Cloud IDMSs. We have further used the proposed taxonomy as an assessment criterion for the evaluation of Cloud based IDMSs.

Results: Our in-depth analysis of various Cloud based IDMSs reveals that most of the systems do not offer support to all the essential features of Cloud IDMS and the ones that do, have their own certain weaknesses. None of the discussed techniques heuristically covers all the security features; moreover, they lack compliance to international standards which, understandably, undermines their credibility.

Conclusion: Presented work will help Cloud subscribers and providers in understanding the available solutions as well as the involved risks, allowing them to make more knowledgeable decisions while selecting potential Cloud IDMSs that best suits their functional and security requirements.

Keywords: Cloud computing security; Identity management; Assessment criteria; IDMS taxonomy

Background

Cloud computing has emerged as a relatively new and influential paradigm for managing and delivering internet-based services and is considered to be an evolution of grid computing, which itself is based on traditional distributed system concepts (Youseff et al. 2008). Cloud computing offers many benefits to the IT industry by offering them unlimited storage and computing capacity. In addition, Cloud is based on pay-as-you-use model that allows organizations to outsource their data and IT services, offering on-demand self-service, broad network access and rapid elasticity at low cost (Mahmood 2011; Wang and Mu 2011). Cloud, being a service oriented computing architecture, is capable of providing anything-as-a-service, including but not limited to Software-as-a-service (SaaS), Platform-as-a-service (PaaS), Infrastructure-as-a-service (IaaS), Database-as-a-service (DbaaS) or Identity-as-a-service (IDaaS). Google (PaaS), Amazon (PaaS and IaaS) and Salesforce (SaaS) are few examples of major Cloud Service Providers (CSP) that offer on-demand and low-cost services/applications to the Cloud Service Consumers (CSC).

Another aspect of the Cloud systems is complexity. The problem in understanding cloud systems stems from the fact that it is simply quite difficult to model them. Cloud is a very dynamic system with numerous users, devices and networks, connecting and disconnecting simultaneously with the cloud. This complexity is to such an extent that it can perhaps be likened to the complexity of a human brain where neurons connect and change their synaptic structure continuously to store information. However, what is a problem here is the fact that unlike the brain, where the connecting neurons are already authenticated, cloud systems require extensive authentication as well as identity management systems. Still, these are simply not enough to cater for the ever-growing requirements of novel paradigms such as the Internet of Things (IoT) in relation to its connectivity with the cloud.

Despite the very attractive features that Cloud promises, the rate of migration to Cloud is rather slow, mainly due to the inherent security challenges associated with the technology. These challenges include data privacy, transparency, risk management, compliance and information security (Fox et al. 2009; Jansen 2011; Subashini and Kavitha 2011). Consequently, the security of Cloud paradigm has become a hot research area, which is being explored by both academic and industrial research communities. In this regard, issues related to the handling and management of sensitive identity credentials have garnered a lot of interest amongst the research communities (Albeshri and Caelli 2010; Chen and Zhao 2012; Gunjan et al. 2012). Storage and processing of identity information by a third party (CSP), outside the organizational boundary, brings in loss of control and transparency issues. This contributes to the reluctance of organizations to move their critical identity information to Cloud.

Cloud based Identity Management Systems (IDMSs) differ from the traditional IDMSs in that they require dynamic governance of provisioning, de-provisioning, synchronization, entitlement, scalability and access control (Gopalakrishnan 2009; Jansen 2011). In addition to this, Cloud IDMSs are required to have updated and synchronized identity information to avoid any conflicts caused by the usage of old user data. Management of sensitive identity information in the Cloud environment raises many privacy and confidentiality concerns. Moreover, security requirements vary from CSC to CSC; therefore,

it is very important to choose the most suitable identity management system that best supports the CSC's security requirements.

An extensive survey on existing Cloud identity management related literature reveals that it is quite dispersed and mainly covers only few specific security features at a time; for instance authentication, authorization and access right delegation etc. Several Cloud identity management systems (Ates et al. 2011; Chowdhury and Noll 2007; Choudhury et al. 2011; Ranchal et al. 2010) have been proposed so far; however, none of those systems holistically meet the requirements of the IT industry, which necessitate a comprehensive identity management system for Cloud. Additionally, to be effective in Cloud, IDMSs are required to incorporate all the essential functional and security features of this paradigm. Furthermore, there exists no benchmark against which one can evaluate existing and newly proposed Cloud identity management systems. As a result, whenever a CSC or CSP needs to opt for an identity management system, they are left unclear about what an IDMS is offering (in terms of their services) and how their security or privacy requirements will be fulfilled.

After reviewing many state-of-the-art Cloud based IDMSs, we present a comprehensive list of attacks that involve identity either as an attack tool or as a target. Keeping in view the potential attacks and security requirements of Cloud IDMSs, we have identified attacks and proposed key features that should be a part of every Cloud IDMS. Presented taxonomy would help IT professionals and researchers understand the importance of these features that are worth considering when implementing or selecting an IDMS for Cloud. We have presented those identified features in the form of a well-organized taxonomy, and have suggested ideal mechanisms for providing said features. As a test case, we have applied the proposed taxonomy as an assessment criterion for the evaluation of existing Cloud IDMSs.

This paper presents a holistic view of identity management domain: a brief introduction about the evolution of IDMSs followed by identity lifecycle management, categories of IDMSs, list of attacks that can be launched against an IDMS, features pertaining to the security of IDMSs in the form of well-informed taxonomy etc. The paper is further organized as follows: Section 'Identity lifecycle management' describes the identity lifecycle management. Further, the novel concept of identity-as-a-service is presented in Section 'Cloud Identity-as-a-Service (IDaaS)'. Evolution of identity management systems is discussed in Section 'Classification of identity management systems', whereas Section 'Open-source cloud platforms & identity management' presents a comprehensive list of well-known open-source Cloud computing platforms and highlight their identity management services and properties. Section 'Cloud identity management: security challenges' highlights many open IDM related security issues and challenges. Well-known attacks against Cloud IDMSs are presented in Section 'Cloud identity management: known attack matrix'. Taxonomy based on the proposed security features is elaborated in Section 'Methods'. Section 'Results' comprises of the evaluation of Cloud identity management systems using the proposed taxonomy. Section 'Discussion' highlights current gaps, challenges and future key-trends related to Cloud identity management systems. Finally, the Section 'Conclusion' highlights the key-points derived out of this study.

Identity lifecycle management

Identity management systems are primarily responsible for the storage, maintenance and retrieval of CSC credentials for either authentication, authorization or some other business functions. The process of identity lifecycle management is the same for Cloud based and conventional systems. Identity lifecycle management encompasses the whole process of identity creation, management of account changes, password management and deletion or de-activation of CSC account in a synchronized manner (Gopalakrishnan 2009), as shown in Figure 1. We have explained each phase of identity lifecycle management in the following subsections.

User Provisioning: Provisioning is also referred to as on-boarding or creation of CSC account by an identity management system (Gopalakrishnan 2009; Meier et al. 2009; Slone 2004). In a Cloud environment, IDMS typically ensure CSC's provisioning via *Just-in-time* or *On-demand* user provisioning techniques. Cloud based IDMSs support provisioning via *Service Provisioning Markup Language (SPML)* or *Security Assertion Markup Language (SAML*) (Maler et al. 2003; Sodhi 2004). When new CSC subscribes for any Cloud service at CSP, IDMS creates his account and stores all the required information. Cloud IDMS assigns identity credentials to the CSC that he uses while acquiring/accessing various Cloud resources. IDMS further defines CSC roles and associates them with certain services to ensure authorized access to the Cloud services, resources and data.

Account changes/management: Over the course of time, CSC might subscribe for other Cloud services or resources; such an activity requires consistent adjustment in the CSC's account information (Gopalakrishnan 2009; Meier et al. 2009; Slone 2004). For instance, if CSC's title or role is changed from Assistant Manager to Manager then the identity management system is required to change the account details accordingly and timely. Other reasons of account modification include change in access privileges or attribute values. Thus, Cloud identity management system is required to accommodate all the changes to CSC account across all the systems in a consistent and synchronized manner. It helps avoid any potential conflicts or security breaches such as unauthorized or illegal access to Cloud resources.

User De-Provisioning: De-provisioning or account deactivation is another important phase of identity life-cycle management (Gopalakrishnan 2009; Meier et al. 2009; Slone

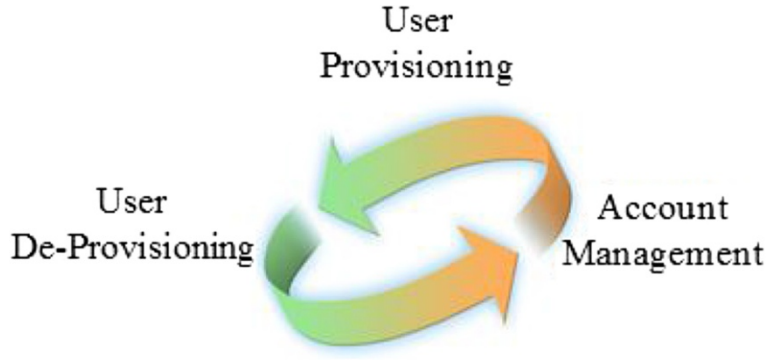

Figure 1 Identity life-cycle management.

2004). In a Cloud environment, de-provisioning means real time revocation that involves a synchronized deletion or suspension of CSC's account along with immediate termination of his access rights from all the organizational services and resources at Cloud. Any delay in de-provisioning could lead to many security risks like malicious use of privileges.

Cloud Identity-as-a-Service (IDaaS)

Cloud Identity as a Service (IDaaS) is essentially the management of identities in the cloud, outside the organizational boundary and applications that use them. The service is provided as third party management of identity functions, including user life cycle management and single sign-on. The term IDaaS is quite broad, and encompasses all three service layers of Cloud computing paradigm including software, platform, or infrastructure; and for both public and private clouds. Hybrid solutions may also exist, whereby identities can still be managed internally within an organization, while other components such as authentication, authorization etc. are externalized through *Service Oriented Architecture (SOA)*. IDaaS besides providing desired identity management services offers all of the Cloud benefits as well, including reduced hardware cost, easy management with wide range of integration options etc. (Rimal et al. 2009; Subashini and Kavitha 2011). For that reason, most of the organizations are moving their existing enterprise IDMSs to Cloud based services.

However, externalizing any portion of identity management functions to third-party provided IDaaS provider may raise several security and privacy challenges as well, which mainly includes *identity data locality, confidentiality, trust establishment, availability* etc. IDaaS may provide a level of benefit to an organization when it comes to functions like account management for an enterprise's SaaS partners, but in the short-term only. Identity management services are still best when managed internally, since, identity management represents the keys to the kingdom and IDaaS vendors don't take on the risk associated with losing critical identity information. Besides that, from an identity management perspective, there are a number of other uncertainties that have arisen with the concept of IDaaS, such as a clear definition of what exactly identity services are and what type of functionality is to be expected, application developers must adhere to SOA requirements, interoperability must be satisfied along with defining an *Application Programming Interface (API)* model that facilitates IDaaS development among many others.

Classification of identity management systems

Identity management systems have actively followed the IT evolution, initiating from Cluster computing followed by Grid and Peer-to-Peer systems that have now transformed into Cloud computing paradigm (Slone 2004; Youseff et al. 2008). Cloud Identity management is a broad, fascinating and continuously evolving domain with some misconceptions regarding its features and services, thus, requiring further investigation. Various Cloud identity management solutions exist and in order to highlight their strengths, weaknesses and suitability for Cloud, we have characterized them on the basis of their *deployment architecture* and *functional behavior*. Figure 2 presents the classification of identity management systems followed by a brief description for each of these systems.

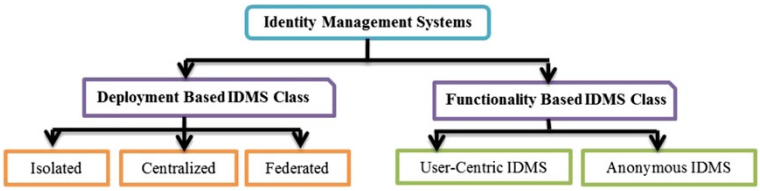

Figure 2 Classification of Cloud Identity Management Systems.

Deployment based classification

Deployment based classification includes the *Isolated, Centralized* or *Federated* identity management architectures. This classification mainly deals with underlying architecture for the storage, management and flow of identity information. Identity information can be stored on a single storage server or it could be distributed across various servers, considering the requirements of CSCs and CSPs.

1. ***Isolated Cloud IDMS*** Isolated Cloud Identity management system is based on the common deployment model used by the small or medium organizations. In an isolated Cloud IDMS, single server acts as a *Service Provider (SP)* as well as the *Identity Provider (IdP)* and is responsible for the storage of identity information and user operations (Alrodhan and Mitchell 2010; Cao and Yang 2010; Jøsang et al. 2005). A common use case is depicted in Figure 3, prior to the service acquisition, (1.1) CSCs are required to perform authentication at the CSP. Here, CSP redirects the user's authentication request to its own IdP for further processing. After successful authentication, (1.2) an authentication response is generated and returned to the corresponding user. This identity management system does not rely on a Trusted Third Party (TTP) for the credential issuance and verification. However, Isolated IDMS becomes unmanageable with the increase in services and resources, since each service needs to know the credentials of authorized users (Cao and Yang 2010; Jøsang et al. 2005).
2. ***Centralized Cloud IDMS*** Centralized Cloud identity management system is slightly different from the isolated IDMS, since it separates the functions of SP and IdP. In a centralized IDMS, a single IdP (a trusted third party) is responsible for the issuance,

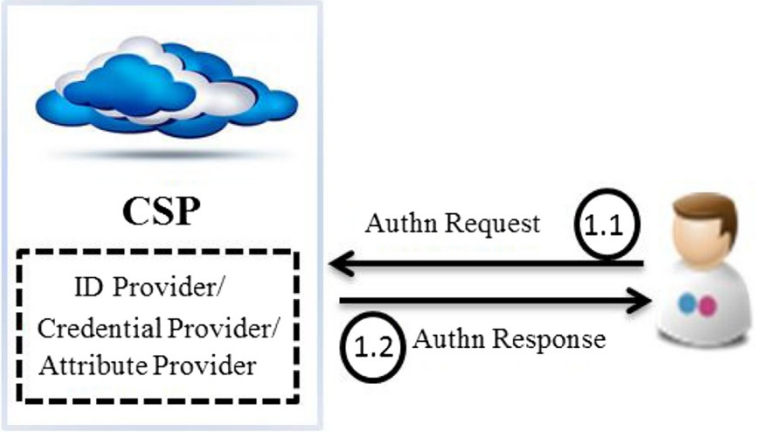

Figure 3 Isolated IDMS.

storage and management of identity data (Cao and Yang 2010; Jøsang et al. 2005; Windley 2005). As a first step, IdP collects all the identity information from CSPs to manage centrally. Later, (1.1) CSC sends an authentication request to CSP, (2.1) Authn request is redirected to the concerned IdP, (2.2) Authn response is sent back to the CSP (1.2) CSC will receive the Authn response (either successful or an error message), as depicted in Figure 4. Typically, single CSC may avail the services of different CSPs that may have a common IdP. In this scenario, CSPs and CSCs are required to have a common trusted IdP since it is responsible for the handling of sensitive identity credentials. An obvious drawback of the centralized IDMS model is single point of failure.

3. ***Federated Cloud IDMS*** Federated Cloud identity management system is the realization of federated identity management model that enables the subscribers of multiple organizations to use the same identification information for acquiring access to all the networks within any particular trusted group of enterprises (Cao and Yang 2010; Chen et al. 2012; Jøsang et al. 2005). Federated Cloud Identity management system has received significant attention from the IT industry because of its design agility that inherently allows cross-domain access to its users by eliminating the need of creating additional user accounts for external parties (Arias-Cabarcos et al. 2012; Shin et al. 2009; Suriadi et al. 2009). Federated IDMS follows the distributed storage architecture, where identity information is stored at multiple locations. The workflow of user request and service provider's response is depicted in Figure 5, where (1) CSC forwards an authentication request to the CSP1, (1.1), the CSP1 being a federated IDMS, forwards the authentication request to the CSP2 for the collection of CSC's identity credentials. As a next step, (1.2) CSP2 forwards the authentication request to the next IdP and retrieves the required attributes from its Identity data store. Finally, an authentication response is created and sent back to the requesting CSP. This process continues until it collects all the attributes required for authentication. In a federated IDMS, CSC's authentication request results in the linking of their information across multiple IdPs, so as to enhance security.

Feature based classification

The functional behavior class includes *Anonymous* and *User-centric* identity management systems. These systems are independent of underlying architecture for instance, a

Figure 4 Centralized IDMS.

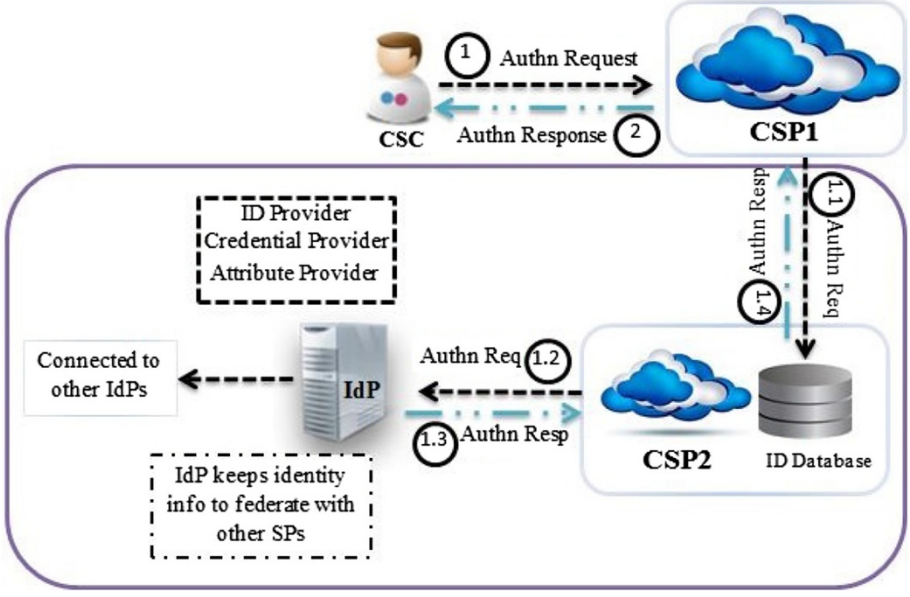

Figure 5 Federated IDMS.

User-Centric IDMS might be based on federated identity management architecture, or it may follow the centralized identity management approach for the management and storage of identity credentials. In the functional behavior class, the key emphasis is on the functionality of the identity management system such as *User-centricity* and *Anonymity*.

1. ***User-Centric Cloud IDMS*** User-centric Cloud identity management system involves user in every identity provisioning transaction. As shown in Figure 6, in order to acquire any service, (1.1) CSCs sends a credential request to the concerned IdP, 1.2) the IdP responses back with all the required credential that are needed to perform authentication. In a User-centric identity management system, CSCs are responsible for the storage, management and retrieval of their personal identity information. It further requires the CSCs to take decisions about the exchange of their identity credentials with other trusted entities such as CSPs, IdPs or users (Alrodhan and Mitchell 2010; Bhargav-Spantzel et al. 2007; Cao and Yang 2010; Suriadi et al. 2009). In

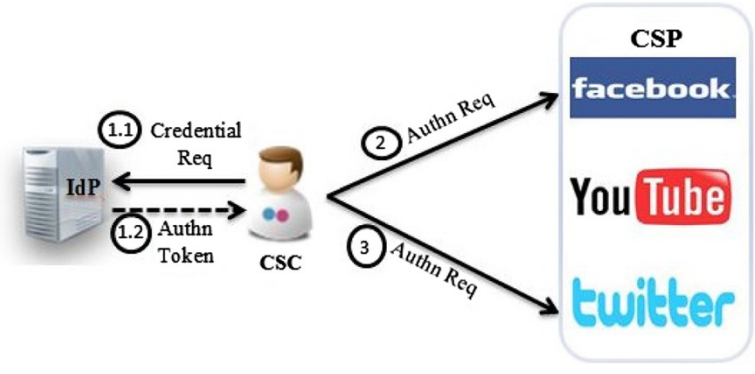

Figure 6 User-centricIDMS.

addition, user-centric IDMSs improve privacy by considering user preferences before disclosing the identity information to the SPs. However, in a service-oriented architecture like Cloud, each application/service requires the CSC to perform authentication and authorization, which is rather cumbersome for the CSC.

2. ***Anonymous Cloud IDMS*** An identity management system that offers anonymity as a feature is termed as an anonymous identity management system. An Anonymous Cloud identity management system is capable of keeping its entity (owner) secret from everyone else (Bhargav-Spantzel et al. 2007; Conrado et al. 2003; McCallister 2010). Anonymous identity should be strong enough to make it hard, if not impractical, to reveal actual identity because data inferred eventually may be connected with other information and can be republished (Bhargav-Spantzel et al. 2007; Conrado et al. 2003). However, anonymous identity management also has some shortcomings, such as lack of trust between the CSCs, and CSPs. It further seems to be negating the purpose of logging and monitoring, since the service consumer is performing actions using some temporary identity.

Open-source cloud platforms & identity management

In this section we present a comprehensive list of well-known open-source Cloud computing platforms and highlight their identity management services and properties.

Eucalyptus - identity & access management

EUCALYPTUS is the acronym for *Elastic Utility Computing Architecture for Linking Your Program to Useful System*, which is an open source private cloud software for building private or hybrid cloud resources for compute, network, and storage that are compatible with *Amazon Web Service (AWS)* APIs (Kumar et al. 2014). I*dentity and Access Management (IAM)* is an authentication, authorization, and accounting system feature within the Eucalyptus private cloud software that is responsible for the management of user identities, enforcement of access controls over resources and providing reports on resource usage as a basis for auditing and managing cloud activities. Eucalyptus by default stores all of the identities and policies in the local *Cloud Controller (CLC)* database (Eucalyptus Identity and Access Management IAM 2012). Identity data can also be pulled from LDAP or Active Directory. The user identity organizational model and the scheme of authorizations are compatible with the AWS Identity and Access Management system with some Eucalyptus extensions that support private clouds. Some of its key benefits include secure credentials management along with efficient and flexible policy based resource access and utilization management.

OpenStack identity service - keystone

OpenStack is an open source cloud computing project that has rapidly become very popular since its first release on October 21st, 2010 (Kumar et al. 2014). OpenStack mainly consist of three core software project which are OpenStack Compute Infrastructure - *Nova*, Object Storage Infrastructure - *Swift* and Image Service Infrastructure - *Glance*. The default identity management system for OpenStack is the OpenStack Identity Service, named as Keystone. Keystone integrates the OpenStack functions for authentication, policy management, and catalog services, including registering all tenants (customer, account, or any organizational unit) and users (person, system, or service), authenticating

users and granting tokens for authorization, creating policies that span all users and services, and managing a catalog of service endpoints (Rhoton 2013). The existing Keystone implementation is centralized, where all users are required to be enrolled in its database, either manually by the OpenStack administrator (via a command line interface or Horizon), or via bulk loading from a corporate database such as LDAP, prior to their access to any of the services. There are a number of well-known limitations with this design, such as users having accounts in multiple systems have to remember multiple credentials for each one.

OpenNebula - users & group management

OpenNebula was first established as a research project back in 2005 and was used by many enterprises as an open and flexible Cloud virtualization infrastructure on their VMware-based data center enabling highly scalable hosting environments (Kumar et al. 2014). OpenNebula includes a complete user & group management system. Users in an OpenNebula installation are classified into four types, *Administrators*, (user belongs to an admin group), *Regular users* (may access most OpenNebula functionality), *Public users* (may access only public interfaces) and *Service users* (user with OpenNebula service account). The resources a user may access in OpenNebula are typically controlled by a permissions system that resembles the typical UNIX one. By default, only the owner of a resource (VM/image) can use and manage it. Users can easily share the resources by granting use or manage permissions to other users in their group or to any other user in the system. Furthermore, OpenNebula comes with an internal user/password authentication system; however, an external authentication driver may also be enabled if required. OpenNebula further supports three customizable authentication configurations; namely, *Command Line (CLI)* (basic user/password, X509, LDAP), *Sunstone* (SSL proxy - Apache) and *Servers* authentication.

Cloud identity management: security challenges

Identity management is a broad domain that involves many open security issues and challenges including *Openness, Identity Theft, Least Privileges, Elevated Privilege Control, Availability, Confidentiality, Integrity, Trust Management* etc (Cloud Security Alliance SecaaS Guidance, Category 1: Identity and Access Management, 2012 by Cloud Security Alliance 2013). Since, technology area such as Cloud Identity Management is still evolving, thus, no well-established standards have been developed so far, resulting in issues like vendor lock-in and lack of openness (availability of specifications/data formats/protocols). *Openness* is critical, so that converters can be developed in the future to ensure interoperability and scalability. Further, since identity information could be accessed by unauthorized or malicious users/intruders. Therefore, adequate security *(encryption, authentication access control, monitoring, etc.)* mechanisms are required to be in place for accessing identity and administration interfaces; otherwise, unauthorized access over the network *(eavesdropping)* would be a key risk factor (Kumaraswamy et al. 2010). In addition to this, Cloud IDMS must subscribe to the principle of *Least Privilege* and proceed using a work-flow mechanism for additional approvals. However, since least privilege not only involves static roles and resources, but also complex context, and dynamic changes (both technical and non-technical). Thus, many Cloud IDMS deployments today enormously over-provision effective access rights to users who even do not

require those access rights. Such excessive access provisioning leads to many critical security issues including unauthorized disclosure, fraud, accidental access and identity theft.

Another most critical aspect of identity management is *Privilege Access Management*. Besides traditional audit and logging requirements, privilege access needs to be a governance mechanism as well. Since, most enterprise applications suffer from mismanagement of roles, violation of segregation of duties, therefore reporting (both success and failure events) on this aspect becomes crucial. Moreover, attacks on identity services or network connectivity, such as *DDoS attacks or resource hogging*, could risk the availability or degrade the performance of an IDMS. If high availability and/or performance are required, redundancy and fail-over options must be considered. Aside from this, due to the ubiquitous nature of Cloud, it is accessible through various devices and applications resulting in an increased number of access points, which sooner or later, adds to the threat of unauthorized disclosure *(confidentiality)* of identity credentials from both insiders (staff) and outsiders (users/intruders) (Mather et al. 2009). Similarly, considering the increased number of access points and system entities, *integrity* of identity data and information stored at Cloud is another important concern which needs immediate attention (Halpert 2011; Lang 2010). In addition to the above-mentioned issues, *management of trust* between the Cloud identity provider and the subscriber is one of the main issues that today's Cloud IDMSs is dealing with. Furthermore, trust is a subjective and context sensitive term which makes it even more difficult to select a Cloud identity provider with fully trusted identity services (Pearson and Benameur 2010).

Cloud identity management: known attack matrix

Currently, a lot of research is focused on Cloud identity management systems; however, security of Cloud IDMSs is an aspect that is still in nascent stages, and requires further exploration. Existing IDMSs are susceptible to various security and performance bottlenecks, which limits their widespread adoption as a potential solution for dynamic Cloud environment. Therefore, we have contributed to this part by conducting a survey on state-of-the-art Cloud based identity management systems and security issues. We present a list of attacks that are either launched against IDMSs or use identity as a principal tool for attack. A brief description of all the identified attacks is presented in Table 1. In addition to this, we have assigned a unique label to each identified attack that we use later in this paper to refer to these attacks. The compiled list aided in determining the key security features that a Cloud based IDMS must provide to ensure the protection and security of Identity credentials in Cloud.

In addition to the attacks, we have also identified the features for Cloud IDMSs that are capable of alleviating the impact of most if not all of the attacks mentioned here. Along with the list of eminent Cloud IDMS features, we have also provided a list of mechanisms that help achieve the identified features. Strengths and weaknesses of each mechanism are also specified wherever required. Cloud IDMS features along with the mechanisms to implement these features is presented in the form of a well-organized taxonomy in the following subsection.

Table 1 Known Attacks against Cloud IDMSs

Label	Attack	Description
A1	Brute-force attack	Brute-force attack generally allows the attacker to gain unauthorized access to sensitive identity credentials of CSCs stored in an identity management server using different possible combinations for user ID and password. Dictionary attack is one example of brute force attack that might be launched against an IDMS if it fails to comply with international standards of strong password settings. Once successful, attacker intensifies their attack in an attempt to uncover the security holes or vulnerabilities of an IDMS. They analyze the server responses and manipulate them to achieve their malicious purposes (Almorsy et al. 2010; Brute Force Attack; Kumaraswamy et al. 2010; Meier et al. 2009; O'Gorman 2003; Ratha et al. 2001; Yassin et al. 2012).
A2	Cookie-replay attack	Here the attacker steals a cookie containing valid session information along with the CSC's identity credentials and reuses it to trick the identity management server into believing that a previously authenticated session is still ongoing and authentic. Through this attack method, attacker may get unauthorized access to victim's (person whose credentials are stolen) confidential information other than Cloud services and resources (Meier et al. 2009).
A3	Data Tampering Attack	It refers to the unauthorized modification of data related to identification of CSC in an identity data-store at Cloud. These modifications may provide the attacker with an opportunity to transgress and damage the Cloud services and resources. This is the attack on the integrity of identity information stored at Cloud mainly due to the loopholes in access control systems (Angin et al. 2010; Meier et al. 2009; Ranchal et al. 2010; Subashini and Kavitha 2011; Thompson et al. 2006).
A4	Denial of Service (DOS) Attack	DoS attack can be launched against an IDMS if it does not provide mechanisms for logging user activities. Since in a DoS attack, attacker overwhelms the Cloud identity management server with false authentication or authorization requests (malformed input data) and tries to either stop the service or consume all of its available resources so that it may not be able to process the legitimate user requests (Almorsy et al. 2010; Meier et al. 2009; Thompson et al. 2006). Therefore, proper logging mechanisms are required to be ensured, so as to make the IDMS intelligent enough to detect and prevent such attacks.
A5	Eavesdropping	This is the attack at communication level, when the Cloud identity management server and CSC exchange the identity credentials for authentication or authorization purpose. It refers to the unauthorized real-time interception and stealing of sensitive consumer information by the attacker either through listening or reading the un-encrypted sensitive data off the network (Bhadauria et al. 2011; Jansen 2011; Jansen and Grance 2011; Jensen et al. 2009; Meier et al. 2009).
A6	Elevation of Privilege	Privilege escalation attack involves legitimate subscribers of the IDMS with limited set of privileges. They illegitimately escalate their access rights by impersonating other CSC that has higher privileges than theirs in order to achieve their illicit objectives and may cause severe damage to the stored information (Meier et al. 2009; Saripalli and Walters 2010; Subashini and Kavitha 2011; Thompson et al. 2006).
A7	Identity Forgery/Cloning/Spoofing Attack	It refers to the unauthorized copying or manipulation of identity tokens or credentials issued from the trustworthy authorities (such as CSP or government), with the intent to deceive or mislead the investigation if followed. Cloud based IDMS should be able to detect the forged identity by implying strict (two-factor) authentication mechanisms. Forged identities further help in committing fraud and identity theft and requires expert knowledge, exceptional skill-set and sometimes much greater effort than the benefits achieved (Chang 2003; Choudhury et al. 2011; Jensen et al. 2009; Kumaraswamy et al. 2010; Meier et al. 2009; Nabeel et al. 2011; Saripalli and Walters 2010; Subashini and Kavitha 2011; Thompson et al. 2006; Zissis and Lekkas 2012).

Table 1 Known Attacks against Cloud IDMSs *(Continued)*

A8	Identity Theft	Identity theft refers to the stealing of someone's identity (such as their name, personally identifiable information, or credit card number), with the intent to acquire Cloud resources or other financial benefits in that victim's name. The victim of identity theft may undergo adverse consequences if they are held responsible for the actions of actual delinquent. In addition to this, identity theft further paves the way for many other crimes such as fraud and forgery (Angin et al. 2010; Ranchal et al. 2010).
A9	Luring Attack	An IDMS that neither ensures user-centricity (such as consistent user experience) nor provides logging & reporting mechanisms is considered to be more prone to luring attack. It is a more specialized form of privilege escalation attack, where the authorized service consumer unknowingly executes the attacker's code fragment in a more privileged security context. More precisely, the adversary targets and 'lures' a high-privileged CSC to perform some illegal activities on their behalf (Angin et al. 2010; Meier et al. 2009).
A10	Phishing Attack	IDMS that offers no support to user-centricity, strong password schemes and privacy preservation considerations is more vulnerable to phishing attack. Phishing is an act of acquiring CSC's information such as name, passwords, social security number, bank account numbers and credit card details by redirecting the CSC to enter his particulars to some replica website whose look and feel is almost identical to the authentic one. Attacker manipulates the communication so that they may appear to be from a legitimate IdP to successfully lure the unsuspicious CSC (Angin et al. 2010; Jansen 2011; Jansen and Grance 2011; Jensen et al. 2009; Kumaraswamy et al. 2010; Olden 2011).
A11	Replay Attack	Replay attack occurs when an IDMS fails to ensure the security of identity credentials during their transmission. In a replay attack, adversary captures the valid identification information and retransmits it, possibly as part of impersonation attack. Unless mitigated, the IDMS subject to the attack, processes user request as an authentic message, resulting in a range of bad consequences, such as unauthorized disclosure of information followed by fraud, forgery and impersonation (Almorsy et al. 2010; Choudhury et al. 2011; Jansen 2011; Jansen and Grance 2011).
A12	Repudiation	Repudiation attack occurs when the Cloud service consumer denies an action. In addition to this, the Cloud IDMS does not implement any controls to maintain service consumer activity logs so no proof exists to prove him accountable for his actions. Due to the absence of real-time tracking and activity logging mechanisms, service consumers can easily repudiate their malicious activities that they have actually performed on Cloud servers, such as unauthorized manipulation of data and forgery of identity credentials (Bertino and Takahashi 2010; Thompson et al. 2006; Yan et al. 2009; Zissis and Lekkas 2012).
A13	Side-Channel Attack	An IDMS may fall victim to side channel attack if it does not follow the principle of federation and access control. As in the side channel attack, attacker steals the information (like session identifiers, timing information, OAuth tokens and electromagnetic leaks) from the physical implementation of a security system. Therefore, it is recommended to deploy a federated IDMS that stores the sensitive identity information in fragments across multiple servers in order to make it hard for the attacker to achieve his malicious objectives (Angin et al. 2010; Bhadauria et al. 2011; Jansen 2011; Jensen et al. 2009; Ranchal et al. 2010; Zhou and Feng 2005).
A14	Skimming Attack	Since skimming is an attack method where criminals steal the sensitive information from authentication tokens (smart card). IDMS should be capable of ensuring strong encryption and secure distribution of identity credentials across multiple servers (Jacobs and Poll 2011; Zissis and Lekkas 2012).
A15	Snooping	Snooping attack permits the illegitimate collection of sensitive information such as identities, available services and network topology from an identity server in Cloud environment. Snooping is slightly different from eavesdropping since it includes more sophisticated surveillance techniques to intercept secret communications such as through remote activity and key-stroke (key-loggers) monitors (Donevski et al. 2013; Salsano et al. 2002).

Methods

Cloud IDMS features & mechanisms: a taxonomy

Having compiled a list of potential attacks against IDMSs, we move on to identifying the most imperative Cloud IDMS features that are required to ensure the security of CSC's credentials. Most of the identified features do exist for traditional IDMSs, but as Cloud brings in new security challenges, we need to revisit them from the perspective of Cloud environment. In this respect, Ferdous et al. in (Ferdous and Poet 2012) have presented a very comprehensive taxonomy covering almost all the functional and non-functional requirements of an identity management system including *usability, trustworthiness, affordability, security* and *privacy*, as shown in Figure 7. However, among all these requirements, security is one key factor that is categorically considered as the most important requirement, and has not been covered in detail thus requires further investigation and exploration. Therefore, in this paper, we have extended their work and provided a well-informed taxonomy (as shown in Figure 8) - that thoroughly covers all the required Cloud IDMS security features and their corresponding mechanisms of realization. Whereas, for other aspects such as *usability, affordability, liability & law enforcement* etc., we affirm the taxonomy presented in Ferdous and Poet (2012) to be reliable and adequate, since it is inclusive of all the crucial requirements. Finally, detailed description of all the identified Cloud IDMS features, along with their mechanisms, is presented in the following subsections.

Authentication

An identity management system has a primary objective of authenticating users or subscribers registered with it. Authentication is the process of verification that ensures whether the person or the application is actually the one or who it claims to be (Jansen 2011; Pashalidis and Mitchell 2003; Shin et al. 2009; Slone 2004; Subashini and Kavitha 2011; Windley 2005; You et al. 2012). In the multi-tenant Cloud environment, users and computer programs are required to prove their identity/legitimacy to the authentication service whenever they attempt to access some application or while acquiring a web resource. Authentication can be provided as a part of an IDMS or it may exist as a separate

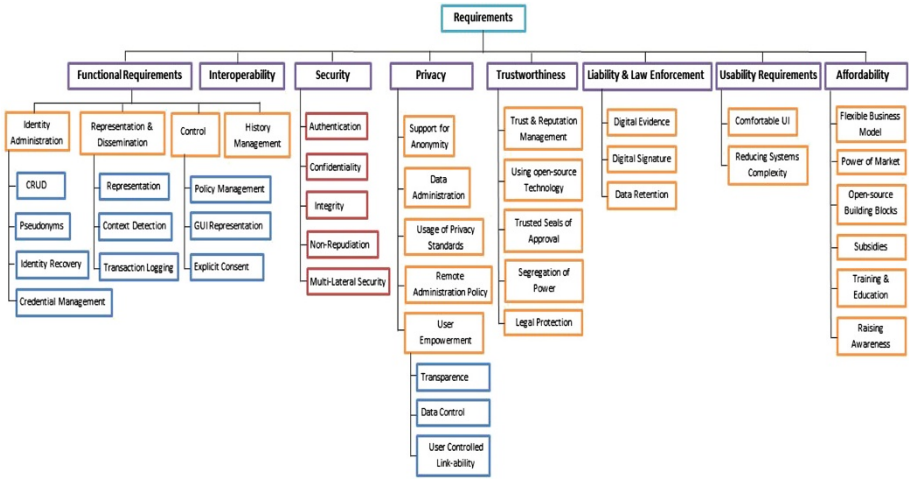

Figure 7 Taxonomy of Identity Management Requirements.

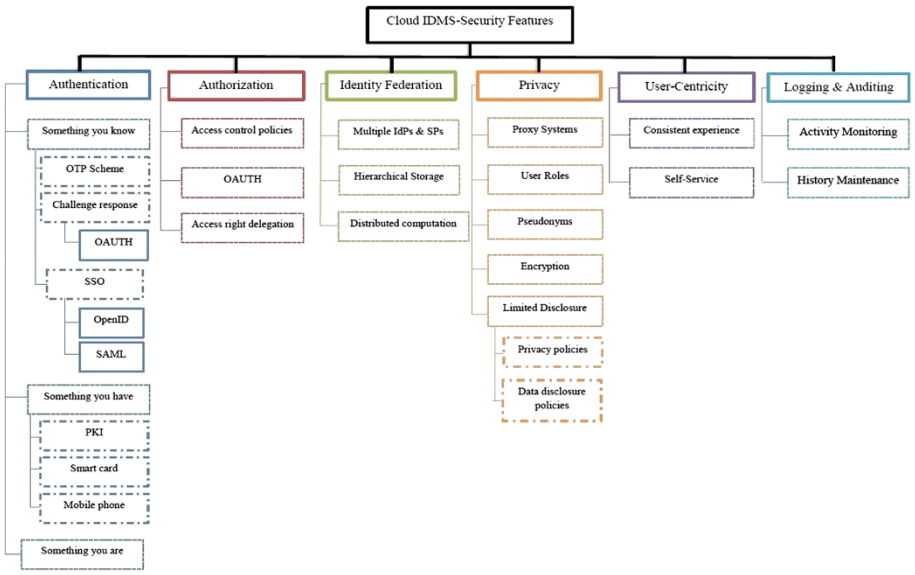

Figure 8 Taxonomy tree of cloud IDMS Components and Mechanisms.

service/system. Authentication commonly relies upon at least one of the factors described below considering the security requirements of the service, since highly secure services require stronger authentication mechanism.

1. ***Something you know*** The conventional and the easiest way of authentication is via password or Personal Identification Number (PIN), something that is shared between the user and the authentication service and is, ideally, both secret and hard to guess. Identity management systems are responsible for the storage, management and secure transmission of user ID and password to the authentication service for verification. In a common Cloud hosted web-service access scenario, user enters his user ID and password/PIN to prove his identity to the authentication server. However, this mechanism is considered to be the least secure authentication mechanism for the dynamic Cloud environment that is susceptible to replay attack and identity theft since user passwords/PIN can easily be stolen. Other reasons might include sharing of passwords or usage of overly simplistic passwords among many others. Password based authentication mechanisms can be enhanced if applied as One-Time-Password (OTP) scheme (Luo et al. 2009; Olden 2011), Challenge-Response mechanism (Choudhury et al. 2011) and Single-Sign-On (SSO) (Ates et al. 2011; Chadwick and Casenove 2011; Choudhury et al. 2011; Kim et al. 2010), each offering different levels of security.

   OTP Scheme: Cloud based IDMS can authenticate users via OTP scheme also (Olden 2011), where user authentication is performed each time with new password that is randomly generated and has no likability to the one used for previous transaction or resource acquisition (Luo et al. 2009). Thus, improves the security and privacy of user during the entire authentication process; however, it decreases the efficiency of the overall system since the authentication system has to generate the OTP and transmit it to the respective user in response to every authentication request.

   Challenge Response Mechanism: In order to make conventional passwords non-reusable and secure, Cloud IDMSs can offer authentication via challenge-response

mechanism (Feng et al. 2010; Ratha et al. 2001; Saroiu and Wolman 2009). Authenticator maintains a list of challenges that are later presented to the user in response to every authentication request. User provides response to those challenges and on the basis of the verification results, user is allowed or denied by the service provider. Challenge-response mechanism also has certain weaknesses as the system is prone to playback/replay attacks and password guessing attacks. Moreover, authentication server is required to have a wide range of challenges each with a unique response, which is hard to achieve practically.

OAUTH: It is an algorithm developed by Initiative for Open authentication and is based on a challenge-response algorithm (Almorsy et al. 2010; Gopalakrishnan 2009; Olden 2011). This algorithm offers one-way authentication as well as mutual authentication, and has digital signatures capability also, so is widely adopted as an authentication mechanism by the Cloud IDMS providers and is widely trusted by CSPs and CSCs.

SSO: In order to facilitate the users, Cloud IDMSs offer SSO capability that does not require its users to remember a large number of passwords. SSO is a onetime assertion or authentication per session/per credential where users can access multiple trusted services or resources at Cloud using a single user ID and password (Chadwick and Casenove 2011; Kim et al. 2010; Pashalidis and Mitchell 2003; Suriadi et al. 2009). Organizations may maintain their independent IDMSs but authentication is provided via unique user credentials. An individual's identity information stored across various identity management systems is linked to those unique credentials while performing authentication. SSO controls access among many interrelated, but autonomous systems (Jansen 2011) and can be achieved via any of the following mechanisms.

(a) **OpenID:** OpenID is an authentication protocol whose main objective is to minimize the number of credentials that a user needs to maintain for the purpose of accessing multiple Cloud services (Angin et al. 2010; Celesti et al. 2010; Gopalakrishnan 2009; Olden 2011; Ranchal et al. 2010). It is a type of federated identity which enables the user to access multiple services using OpenID credentials instead of service specific user name and password. OpenID, on behalf of user, requests the service provider for the required service. Moreover, it eliminates the chances of password disclosure, since no OpenID-based Cloud service actually stores user's password information.

(b) **Security Assertion Markup Language (SAML):** SAML is an open standard framed by OASIS for the representation and exchange of identity information among various trusted CSPs while performing user authentication or identification (Celesti et al. 2010; Gopalakrishnan 2009; Jensen et al. 2009; Maler et al. 2003; Olden 2011). SAML version 2.0 offers support to web SSO using token, containing user identity information, that is issued by the IdP. These tokens are recognizable to various trusted CSPs while performing user authentication in response to the user's SSO request.

Since, it is impractical to eliminate passwords from the authentication mechanisms, their security can be further enhanced if they are used in conjunction with other authentication factors and technologies such as biometrics or smart cards.

2. ***Something you have*** Identity management systems can also offer authentication on the basis of *"something you have"* that is commonly referred to as token-based authentication and is a comparatively stronger authentication mechanism. The secret user authentication credentials are encoded in hardware or software tokens that are verified against the information stored by the corresponding IDMS prior to the access of every web service/resource. However, authentication-tokens individually are also vulnerable to identity theft attacks since these cards can be lost or stolen and the adversary can use them for their own malicious purposes. The security of this authentication mechanism can be enhanced by combining it with *"something you know"* for instance a PIN code or password. Token-based authentication can be realized via any of the following methods:

   Public Key Infrastructure(PKI): Identity management systems are capable of accepting digital certificates as software authentication tokens issued by the trusted certification authority (CA). Authentication server traces back the certificate to the issuing party in order to ensure the legitimacy of the user presenting the certificate.

   Smart Card: SecureID tokens or smart cards are also accepted as valid authentication tokens by various IDMSs as smart cards are capable of storing long and hard to recover secret user information (Cameron 2005; Ratha et al. 2001). Smart cards are designed to be tamper resistant. Users present the smart card to the authentication service that verifies the encoded information from its identity management database before sanctioning the user to access any web service or resource.

   Mobile Phone: Identity management systems may incorporate cellular devices (mobile phone) having a SIM (Subscriber Identification Module) card to connect the users to the authentication service via mobile network (Ratha et al. 2001). Mobile phone network is used to communicate the authentication information (password) between the user and the authenticator via SMS (Short Message Service). Authentication information can be voice confirmation from the user or OTP send by the server that the user enters afterwards to verify the legitimacy of user.
3. ***Something you are*** The final category of authentication that an IDMS can support is based on biometrics where user verification is performed on the basis of some natural characteristics such as fingerprint, voice patterns, or iris characteristics that are unique for every individual (Jensen et al. 2009; Leandro et al. 2012; Senk and Dotzler 2011).

To make the authentication system stronger, any two of the aforementioned factors can be combined as two-factor authentication, which is considered highly secure. Most commonly *"something you have"* is combined with *"something you know"* e.g. smart card along with a PIN is used to authenticate a user more securely in Cloud IDMSs.

Authorization

Authorization plays an important part in Identity management system; authorization is the process of granting and denying access to any web resource and service (Slone 2004; Subashini and Kavitha 2011; Windley 2005; You et al. 2012). The authorization process decides what a subject (users or applications) is allowed to do on the system and this decision is taken by using subject's identity information. Cloud is a multi-provider environment where one user might have access to multiple services each can be from a different provider having different security levels. Therefore, Cloud

service providers are required to ensure effective authorization for their resources and services in every possible situation. Authorization in a Cloud environment is commonly achieved via access control policies, defined and implemented by the CSPs for their subjects (CSCs), so that only authorized subject may accesses the services and resources.

Access Control Policies (ACP): Cloud service providers implement access control policies on top of identity management systems to ensure that only the legitimate users acquire/access the services and resources they offer (Ates et al. 2011; Chadwick and Casenove 2011; Chowdhury and Noll 2007; Hoellrigl et al. 2010). Complete knowledge about 'Who' can access 'What' and 'When', gives a clear picture of the security and protection of CSP's resources/services. Accordingly, CSPs can take effective security measures to make illegitimate use, unauthorized modification and disclosure of their services, relatively hard if not impractical.

Access Right Delegation: In an IDMS, delegator (person who wants to delegate his access rights) may want to delegate his access rights of some Cloud based web-service to some delegatee (person who receives the delegation) as desired by the delegator or delegatee (Gopalakrishnan 2009; Hoellrigl et al. 2010; Li et al. 2010; Zissis and Lekkas 2012). Delegation of access rights is typically based on any of the access control models, such as Role based access control (RBAC) or Attribute based Access Control (ABAC), where each model specifies a different mechanism for delegation. For instance, in RBAC, access permissions are granted to a role that is later linked to the concerned delegatee. However, in the process of delegation, delegator is required to protect his privacy by restricting the delegatee (via access control policies or privacy policies) from accessing any additional identity information of the delegator.

OAUTH: OAUTH is an open standard for authorization; it allows the service consumers to access the CSP's services or resources on the behalf of the resource/service owner (Almorsy et al. 2010; Gopalakrishnan 2009; Olden 2011; Sanchez et al. 2012). OAUTH follows the principle of access right delegation where resource owners delegate access rights to service consumers without sharing their identity credentials (such as user-ID and password pair). In a common OAUTH scenario, the CSC first accesses a service/application that redirects him to the IdP, where he performs authentication and after successful authentication, IdP redirects the service consumer back to the Cloud service along with the identity token. From then on, service consumers access that particular service via that token.

Identity federation

Identity management systems may offer support to identity federation that enhances the security of identity information during the transmission and storage of credentials. Identity federation has two meanings: it can be a method of associating and communicating a person's digital identity and attributes that are stored across multiple Cloud based IDMSs or it could be any standard, contract and technology that make the identity information movable across independent domains (Arias-Cabarcos et al. 2012; Chen and Zhao 2012; Shin et al. 2009; Slone 2004; Suriadi et al. 2009). Identity federation plays the key role in securing user credentials while moving towards the Cloud. Identity federation can be achieved via any of the following mechanisms:

Multiple IdPs and SPs: An IDMS might involve multiple IdPs and CSPs for the storage and processing of service consumer's identity information (Celesti et al. 2010; Chadwick and Casenove 2011; Hoellrigl et al. 2010). In other words, the identity credentials of a single service consumer are stored at multiple Cloud servers in small chunks following the distributed architecture. Consequently, while performing authentication, authenticator collects the identity information from all the relevant IdPs and CSPs and processes them as required.

Hierarchical Storage: Identity information stored in hierarchical fashion either on a single server or on multiple nodes (typical Cloud scenario) is considered to follow the identity federation principle (Yan et al. 2009). Hierarchical storage offers different levels of access and improves the information accessibility and security. In the hierarchical storage, IDMSs store user information with different access levels considering the sensitivity of identity credentials; therefore, in case if any intermediate node gets compromised, the impact of information loss will be minimal.

Distributed Computation: Distributed Computation: IDMSs are said to be following the identity federation principle, if they follow the distributed processing architecture for user authentication. The distributed architecture works by disseminating the identity information among multiple Cloud servers for the computation or verification of user credentials. This approach accelerates the authentication process and improves security (Ates et al. 2011; Chowdhury and Noll 2007; Kim et al. 2010; Ranchal et al. 2010).

Privacy

Identity management systems are meant to store and process sensitive user credentials that the user wants to protect from unauthorized or unwanted disclosure (Bhargav-Spantzel et al. 2007; Cameron 2005; Leskinen 2012; McCallister 2010; Windley 2005). Privacy is among the top most concerns of users while storing or sharing their secret identity information for either e-commerce or other purposes. Moreover, storage of sensitive identity information in the Cloud, which is outside the organizational boundaries and beyond the user control, elevates user's privacy concerns. Listed below are the mechanisms through which identity management systems can guarantee user privacy:

Proxy systems: Proxy can be a Cloud service or server that personifies someone else (user/application) and acts on their behalf. Identity management systems assign a unique credential to almost every entity be it a system, resource or a service consumer, thus raising privacy concerns (Ates et al. 2011; Olden 2011; Wang et al. 2010). Proxy is particularly intended to enhance user's privacy by requesting the desired Cloud resource/service on behalf of its registered users/systems. The identifying information that is forwarded, for either authentication or resource acquisition, is of the Cloud proxy system rather than the actual user who has requested for the service.

User Roles: A single user might have multiple contextual identities such as personal (name, e-mail ID), social, professional (employee-ID, Salary), and citizen (for instance National ID card), each with different security requirements (Ates et al. 2011). In order to ensure user's privacy while accessing multiple Cloud services, only relevant identity attributes must be shared. An IDMS should be capable of understanding and specifying separate user roles so that only required and related information is forwarded to the respective CSP.

Pseudonym: Pseudonym is a temporary name that is generated either by an IdP upon user request or by the users themselves, whenever they need to protect their privacy while accessing a Cloud based web service/resource (Luo et al. 2009; Zhang and Chen 2010). Pseudonyms intend to protect an individual's true identity in an online transaction. It is recommended to use a different pseudonym for every different Cloud service so that they cannot be linked to the user's original identity.

Encryption: Encryption is used to convert the identity information into some unintelligible form so that even if disclosed, information might not be useful to the adversaries (Chadwick and Casenove 2011; Kim et al. 2010; Nabeel et al. 2011). In order to ensure privacy, Cloud based identity management systems must offer encrypted storage and transmission of identity credentials. The key used for the encryption of identity credentials is securely shared between the communicating parties only so that the information will only be disclosed to the authorized user having the right key pair.

Limited Disclosure: The best practices regarding identity management dictates that information should be disclosed on a *"need to know"* basis, and stored on a *"need to retain"* basis, as that may help to ensure the minimal damage in the event of any violation such as theft of identity information (Cameron 2005).

1. **Privacy Policies:** Identity management systems implement privacy policies to protect their service consumer's identity information in accordance with their preferences. Identity disclosure policies are specified and implemented at the service consumer end (Angin et al. 2010; Celesti et al. 2010; Chowdhury and Noll 2007; Choudhury et al. 2011; Ranchal et al. 2010; Yan et al. 2009. CSCs (data owner) demand transparency about 'who' wants to access 'what' part of their identity information. Whenever CSC attempts to access or acquire a Cloud service/resource, CSP needs certain amount of identity information to verify his authenticity. Therefore, before forwarding CSC's credentials to the CSP, identity management system must consult the privacy policies or may ask for the CSC's consent prior to identity information disclosure. It enables the CSC to decide whether they want to acquire that resource by sharing their identity information with the CSP or if they would prefer to protect their privacy so that they may withdraw their resource acquisition request.
2. **Data disclosure policies/preferences:** Commonly, user-centric IDMSs offer consistent user experience by allowing the user to select the credentials and attributes from identity attribute lists issued by the IdP, in advance, to each operation (Hoellrigl et al. 2010; Zhang and Chen 2010). Service consumers may also specify their identity revelation rules prior to actual service usage to ensure the security and privacy (Fox et al. 2009; Hoellrigl et al. 2010; Zhang and Chen 2010) of their information. User centric IDMSs allow its users to choose an IdP of their own choice which they believe is more appropriate for any particular transaction thus, places greater responsibility in the hands of users.

User-centricity

User centricity is an important identity management feature which emphasizes on transferring the control of identity attributes and disclosure preferences in the hands of identity possessor (CSC). In a user-centric IDMS, CSCs are involved in every identity provisioning operation and have full control over their online identity information (Dhamija and

Dusseault 2008; Leskinen 2012; Windley 2005). CSCs are responsible for the management of their identity credentials; however, user-centric systems have problems in terms of security and privacy. Following are the mechanisms through which identity management systems provide user centricity to the Cloud service consumers.

Consistent User Experience: Identity management systems are required to offer support to various technologies (e.g. OpenID, SAML, OAuth) run by multiple IdPs to ensure the interoperability among various systems (Cameron 2005; Celesti et al. 2010; Chowdhury and Noll 2007; Ranchal et al. 2010). An IDMS that supports interoperability among various identity management systems (by either offering support to multiple technologies or by following common schema for the exchange of identity credentials) help to ensure consistent user experience while accessing multiple services.

Self-service: Identity management systems are required to provide a self-service feature that enables the user to alter his sensitive personal information stored by the Cloud service providers (such as postal address, phone number, password etc.) (Ates et al. 2011; Choudhury et al. 2011; Luo et al. 2009). Users must be allowed to modify/update their personal identification information that uniquely identifies them in an IDMS. It also reduces the SP's operational costs and troubleshooting time.

Logging & auditing

Identity management systems incorporate logging and auditing feature that helps to ensure the proper working of identity management system and gain the trust of its customers/users in the system (Bhargav-Spantzel et al. 2007; Windley 2005). In a multitenant Cloud environment, it is comparatively harder to identify the person responsible for any security breach or misbehavior. Therefore, Cloud IDMSs are required to provide logging and auditing facility that compliments the security of Cloud applications and identity management system both. Generally, Cloud SPs are more concerned about the maintenance of logs such as recording of all sensitive user activities (authentication requests forwarded to an IDMS). Logs help in identifying the person responsible for any security breach, thus, accordingly the legally responsible person is penalized for his actions. Whereas, auditing is of mutual interest to the CSCs and CSPs, auditing at one end help CSPs in making sure that their systems/services are in line with their business objectives. On the other hand, auditing highlights the security loopholes that the service consumer needs to know and upon which he either makes his decision of electing the IDMS. Logging and auditing can be achieved via any of the mechanisms mentioned below:

Activity Monitoring: Identity management systems may offer auditing and logging via user activity monitoring functionality (Ates et al. 2011). Often system administrators in Cloud come across situations when they need to answer "Who did it?" though that happens fairly less, but those events are critical. In order to get ahead in security and to timely identify system misuse and user misbehavior, monitoring should be a necessity. An IDMS offers monitoring by tracking and storing each user action or web access in the log files that are later used for auditing purposes.

History Maintenance: Identity management systems might incorporate history maintenance module for maintaining the history of all user actions (such as web access) and attribute exchanges among the service consumers, IdPs and CSPs (Angin et al. 2010;

Ranchal et al. 2010). History maintenance module benefits the CSPs by preserving the user activity logs thus in case of any security breach the wrongdoer can be identified appropriately. Whereas, Cloud service consumers are benefited by the storage of attribute sharing history that helps them in making future attribute disclosure decisions whenever they access the same service or resource again.

There is a strong association between the above-mentioned security features and the attacks presented in Section 'Cloud identity management: known attack matrix'. Each of these mechanisms is capable of mitigating one or more attacks that could be launched against a Cloud IDMS. In order to provide better understanding, we have summarized our findings in Table 2, which depicts a clear mapping between the identified features, mechanisms and the attacks they can mitigate. For instance, if a Cloud IDMS offers **Authentication** using *Biometrics*, then it is capable of mitigating attacks such as brute-force (A1), dictionary attack (A6), forgery (A10), impersonation/identity spoofing (A13) and repudiation (A17), since biometrics involve natural characteristics (such as fingerprint, voice patterns etc.) that are unique for every individual and hard to counterfeit. Similarly, if a Cloud IDMS follows **Identity Federation** principle through *Hierarchical Storage*, then it will limit Unauthorized disclosure of confidential data (A7), Elevation of privileges (A9), Forgery (A10), Identity theft (A12) and Impersonation attack (A13), as the information will be stored in fragments across multiple servers. Therefore, although the attacker somehow manages to compromise one Cloud identity management server and accesses its stored information even then they are unable to launch any attack because all they can acquire is partial information that is simply insufficient to perform the attack.

Table 2 Relationship b/w Features, Mechanisms and Attack Matrix

Features	Mechanism	Mitigated attacks
Authentication	Something You Know (OTP & CR)	A2, A5, A6, A7, A10, A11, A12
	Something You Have (Tokens)	A5, A14
	Something You Are (Biometrics)	A1, A4, A5, A12
Authorization	Access Control Policies	A3, A6, A13
	OAuth	A5, A6, A7, A8, A10, A11
	Access Right Delegation	A3, A6
Identity federation	Smart-card (Encryption)	A5, A12
	Multiple `IdP`s and `CSP`s	A7, A8, A13, A14
	Hierarchical Storage	A6, A7, A8
	Distributed Computation	A15
Privacy	Proxy-systems	A8
	User-roles	A6
	Pseudonyms	A8, A10
	Encryption	A5, A7, A8, A10, A14, A15
	Limited Disclosure	A6, A7, A8
User-centricity	Consistet Experience	A9, A10
	Data Disclosures Policies	A3, A6, A9, A13
Audit & Logging	Activity Monitoring	A1, A4, A12
	History Maintenance	A9, A12

Results

Analysis of cloud identity management systems

Taxonomy, presented in Section 'Methods', is being used here as an assessment criterion for the evaluation of existing IDMSs. The objective of our analysis is to assist CSCs and CSPs in selecting the most appropriate IDMS that best suit their functional and security requirements. We have critically analyzed various Cloud based identity management systems; Table 3 provides a brief overview of the reviewed systems and their important technical features. In addition to this, identity management systems from each category (Deployment based, Featured based) have been analytically evaluated against the IDMS features discussed above and findings from the analysis are presented at the end of this section in Tables 4 and 5.

Deployment based classification

1. ***Isolated IDMS***

   – ***A Strong User Authentication Framework for Cloud Computing:*** Choudhury et al. (2011) propose a strong user authentication framework that conforms to the Isolated IDMS properties, where single Cloud SP is responsible for the storage, maintenance and verification of identity credentials and does not rely on any trusted third party (IdP). Proposed framework uses *smart card* based on bilinear pairings and *user password* to provide **two-level Authentication**, in order to avoids illegitimate access to Cloud resources and data. The framework offers **User-Centricity** by offering support to *self-service* feature via password change facility specified in the system design. The proposed secure Cloud framework ensures user **Privacy** via *limited disclosure principle* by using two separate channels for the transmission of sensitive user credentials that minimizes the impact of information disclosure and ascertain protection against identity theft attacks. Distribution of credentials is achieved in a way that some information is stored in the user's smart card, whereas *one-time key (password)* is sent by the server to user's mobile via SMS, thus offering support to **Identity federation** as well. However, the system specifies no **Authorization** mechanism. Furthermore, the design of proposed framework falls short, as far as **Auditing and Logging** is concerned.

   – ***Protection of Identity Information in Cloud Computing without Trusted third party:*** Ranchal et al. (2010) has described a security solution for Personal Identity Information (PII) that prevents unauthorized disclosure and usage of user's sensitive identity information. Proposed scheme ensures user **Privacy** via AB, which discloses restricted PII to the SP following the *limited disclosure* principle, and provides security against identity attacks. AB scheme offers **User Centricity** by incorporating 'Disclosure Policy' component through which users can specify policies for their data. *Disclosure policy* component ultimately ensures the security of their sensitive information accumulated at the Cloud SPs and offers a *Consistent user experience* across multiple SPs. Another significant feature of AB scheme is 'Identity Data', which stores encrypted identity information that is later used for secure user **Authentication**. 'Disclosure History' is yet another important feature of AB scheme which offers *history maintenance*, and is later used to carry

Table 3 Key Features of Cloud IDMSs

Type	Cloud IDMSs	Salient features
	Deployment Based Cloud IDMS	
Isolated IDMS	A Strong User Authentication Framework for Cloud Computing (Choudhury et al. 2011)	- Conforms to isolated IDMS properties - Offers security and privacy of user by restricting illegal access - Mutual authentication (Challenge Response & OTP scheme) - Secure session key generation and distribution - Multi-factor authentication (Password and smart-card).
	Protection of Identity Information in Cloud Computing without Trusted third party (Ranchal et al. 2010)	- Isolated IDMS, since it does not rely on any trusted third-party - Protects PII against unauthorized disclosure - Computes assertions over encrypted data - Active bundle scheme for un-trusted hosts - Encrypted storage of identity data
Centralized IDMS	An Identity-Centric Internet: Identity in the Cloud, IDaaS and other delights (Ates et al. 2011)	- Realization of centralized Cloud IDMS - Defines the concept of Identity in Cloud Agents (IC-Agents) - IC-Agents as an identity proxy perform identity propagation transactions - Explains the IDaaS module in the context of Personal Data-as-a-Service - Authentication and Authorization as-a-Service module
	Distributed Identity for Secure Service Interaction (Chowdhury and Noll 2007)	- Presents a role based IDMS architecture - Categorizes digital identity as Personal, Corporate and Social identity - Restricted disclosure of identity credentials to the CSPs - Centralized IdP is responsible for the sharing and distribution of user's identity credentials
Federated IDMS	Security and Cloud Computing: ICIMI (Celesti et al. 2010)	- Inter-Cloud Identity Management Infrastructure (ICIMI) is a federated IDMS - Allows for the expansion of virtualization infrastructure - Establishment of trust among CSPs - Offers standardized, scalable & dynamic authentication
	Strengthen Cloud Computing Security with FIM Using HIBC (Yan et al. 2009)	- Allocates unique identities in hierarchal fashion - Mutual authentication for Hybrid Cloud environment - Handles the establishment of secret session keys
	Chord Based Identity Management for e-Healthcare Cloud Applications (Kim et al. 2010)	- SSO service for Cloud based e-Healthcare application - Uses Peer-to-Peer service model for load balancing - Distributes session information in the federated Cloud environment - Limits the number of authentication requests to central IdP
	Security APIs for My Private Cloud (Chadwick and Casenove 2011)	- Federated access rights to Cloud resources - Proposes Authz API for maintaining the identity database and defining the access control mappings - Authn API for authenticating the Cloud users - Delegation API to delegate access rights to anyone at any time

Table 3 Key Features of Cloud IDMSs *(Continued)*

Functionality Based Cloud IDMS		
	An Identity-Based OTP Scheme with Anonymous Authentication (Luo et al. 2009)	- Identity based One-time Password (OTP) authentication scheme
		- Operates on smart card based bilinear pairings
		- Generates a temporary identity to protect user's actual identity
		- Describes Process Setup and User Registration module
		- Guarantees user's anonymity and privacy throughout the communication process
Anonymous IDMS	UIMM Based on Anonymous Credentials (Zhang and Chen 2010)	- Universal Identity Management Model (UIMM) that operates on anonymous credentials
		- Allows for access right delegation
		- Ensures user's privacy preservation via unlikable self-generated pseudonyms
		- Extend WS-Federation to implement Identity Meta-system model.
	An Entity-centric Approach for Privacy and Identity Management in Cloud Computing (Angin et al. 2010)	- Entity-centric architecture for Identity Management in
		- Implements Active Bundles (AB) scheme to ensures user's anonymity
		- AB encapsulates Personal Identity Information (PII), Privacy preserving rules and VM (Virtual Machine)
		- Implements anonymous identification
	(Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing (Sanchez et al. 2012)	- Dynamic privacy-enhanced federated identity management solution that defines an enhanced privacy
		- Introduces a new reputation protocol and implements Enhanced Client Profile (ECP)
		- Presents Trust aware IDM architecture that mainly comprises of Identity Management (IdM) layer and Trust layer
		- IdM Layer facilitates user authentication, authorizations and profile management
		- Trust layer deals with the management, negotiation and distribution of trust related data to other layers.
User-Centric IDMS	User-Controlled Automated Identity Delegation (Hoellrigl et al. 2010)	- Implements Identity Delegate that applies user defined data disclosure policies and resolves the information consistency problem
		- Allows for the integration of multiple IdPs and SPs
		- Dissemination of identity credentials is kept under the control of the identity owner

out auditing, thus offering support to **Auditing and Logging** principle. This scheme eliminates the need of a TTP for the handling of identity management functions as it follows the *distributed storage and computation* mechanism by distributing the secret identity information among multiple nodes to ensure security as well as **Identity Federation**. However, **Authorization** is not included in the proposed solution for the assurance of appropriate access control to the appropriate applications.

Table 4 Analysis of Deployment based IDMSs

Categories	Cloud IDMSs	Authn	Authz	Identity Federation	Privacy	User-Centricity	Audit & Logging
Isolated IDMS	A Strong User Authentication Framework for Cloud Computing (Choudhury et al. 2011)	Smart card + OTP	–	Mobile phone + Smart Card	Limited Disclosure	Self-Service	–
	Protection of Identity Info. in CC without TTP (Ranchal et 2010)	–	–	Distributed Computation	Limited Disclosure	Consistent Experience	History Maintenance
Centralized IDMS	An Identity-Centric Internet: Identity in the Cloud, IDaaS (Ates et al. 2011)	SSO	Access Control Policy	Distributed Computation	User Roles	Self-Service	Activity Monitoring
	Distributed Identity for Secure Service Interaction (Chowdhury and Noll 2007)	Mobile phone + Pwd	Access Control Policy	Distributed Computation	Limited Disclosure	Consistent Experience	–
Federated IDMS	Security and Cloud Computing: ICIMI (Celesti et al. 2010)	SSO	–	Multiple IdPs	Limited Disclosure	Consistent Experience	–
	Strengthen Cloud Computing Security with FIM Using HIBC (Yan et al. 2009)	SSO	–	Hierarchical Storage	Limited Disclosure	Consistent Experience	–
	Chord Based Identity Management for e-Healthcare Cloud Applications (Kim et al. 2010)	SSO	–	Distributed Computation	Encryption	Consistent Experience	–
	Security APIs for My Private Cloud: granting access to anyone (Chadwick and Casenove 2011)	SSO	Access Control Policy	Multiple IdPs	Limited Disclosure	Consistent Experience	Activity Monitoring

Table 5 Analysis of Deployment based IDMSs

Categories	Cloud IDMSs	Authn	Authz	Identity Federation	Privacy	User-Centricity	Audit & Logging
	An Identity-Based OTP Scheme with Anonymous Authentication (Luo et al. 2009)	Smart card + OTP	–	Smart Card	Pseudonyms	Self-Service	–
Anonymous IDMS	UIMM Based on Anonymous Credentials (Zhang and Chen 2010)	–	Access Control Policy	–	Pseudonyms + Data Disclosure Prefer.	–	–
	An Entity-centric Approach for Privacy & IDM in Coud Computing (Angin et al. 2010)	–	–	–	Limited Disclosure	–	History Maintenance
User-Centric IDMS	Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing (Hoellrigl et al. 2010)	PKI	OAUTH	–	–	–	–
	User-Controlled Automated Identity Delegation (Sanchez et al. 2012)	User name + Pwd	OAUTH + Access Control Policy	Multiple IdPs	Data Disclosure Prefer.	–	–

2. ***Centralized IDMS***

   – ***An Identity-Centric Internet: Identity in the Cloud, IDaaS and other delights:*** Concept of Identity in Cloud Agents (IC-Agents) is presented in Ates et al. (2011), which is a logical identity proxy with Identity as a Service (IDaaS) component. The proposed concept of logical identity proxy (IC-Agent) ensures the segregation of user's PII while disseminating user's credentials across multiple SPs. Moreover, IC-Agents acquire *user consent* before disclosing their sensitive identity information mandatory for the verification process thus offering support to **Privacy** feature. Moreover, IC-Agents are capable of *monitoring and logging* all the operations of user (for instance authorizations and other service accesses), which may help to carry out the auditing processes as per SP's requirement, thus offering support to **Auditing and Logging** principle. Furthermore, IC-Agents provide interfaces called dashboards for user **Authentication** and are capable of functioning as a personal IdP to provide *SSO* facility that eliminates the need of repeated user logins for each independent resource access. IC-Agents is a **User-Centric** identity management concept where users are provided with full control over their identity information stored at IC-Agent host (Software and Hardware) by offering support to *self-service* mechanism. Proposed concept of IC-Agent is based on the *distributed storage architecture* for personal data storage where some data is stored by the IC-Agent, while other information is retrieved from multiple distinct IC-Agent sources thus follows the **Identity Federation** principle. IC-Agent applies the user defined *data disclosure policies* while forwarding user credentials to the SPs for secure authentication and **Authorization**.
   – ***Distributed Identity for Secure Service Interaction:*** Chowdhury and Noll (2007) present a Role based identity management architecture that utilizes users' mobile devices as unique attributes of their digital identity. Presented architecture ensures user's **Privacy** by following the *limited disclosure* principle, where each identifier discloses limited information to the SP while accessing multiple related services. System complements user privacy even more by accepting the segregation and distinction among the different identity contexts such as personal, social and corporate identity. **Authorization** is provided through role based access control model that implements *access control policies* considering user roles. The **Identity Federation** mechanism is ensured via *distributed storage and computation* mechanism, which distributes the identifying information across multiple locations, for instance partial user credentials are held in the network storage area, whereas the other half is stored at the user's mobile device (SIM card). Proposed system offers **User Centricity** since it offers *self-service* feature via my digital identity component that allows the user to alter, append or revoke his stored identity credentials. Moreover, network based identity data store (My digital identity) enables the user to define *data disclosure policies* that guarantees seamless and *consistent user experience* across multiple SPs. System provides **Authentication** via user's SIM card so belongs to the *"something you*

have" authentication mechanism; the system also proposes an extended SIM card architecture that holds multiple credentials for different authentication services. However, the system does not specify any **Auditing and Logging** functionality that is critical for maintaining and keeping the check and balance on CSCs as well as Cloud SPs for the security of IDMSs.

3. ***Federated IDMS***

   - ***Security and Cloud Computing-ICIMI:*** Inter-Cloud Identity Management Infrastructure (ICIMI) is described in Celesti et al. (2010), which is a federated IDMS. ICIMI uses IdP/SP model to provide **Authentication**, where Home Cloud performs one-time authentication to access the federated Foreign Cloud services that are in its shared trusted domain thus follows the *SSO* mechanism. This infrastructure offers support to **User-Centricity** by providing a solution that offers *consistent user experience* since it is independent of the underlying authentication mechanisms and incorporates standards such as SAML, which is capable of accepting assertions having different formats. Moreover, ICIMI is based on *distributed system architecture* comprising of multiple IdPs; therefore, the mechanism for storage and retrieval of user credentials follows the **Identity Federation** principle. In addition, this scheme offers **Privacy** via *limited disclosure principle* where Home Cloud hides the identity of CSCs by making the resource acquirement request on behalf of its consumers (users). However, the system incorporates no **Authorization** or access control mechanism that ensures legitimate access to Cloud services and resources. Secure logging to ensure **Auditing and Logging** is another significant feature of IDMSs but is not reflected in the design and architecture of the proposed infrastructure.
   - ***Strengthen Cloud Computing Security with FIM Using HIBC:*** A Federated Identity Management (FIM) system for Cloud along with Hierarchical Identity-Based-Cryptography (HIBC) is described in Yan et al. (2009), which allocates unique identities to users and servers in hierarchical fashion. This system provides **Authentication** via *SSO* mechanism that requires the user to use single identity credentials for accessing multiple services and resources that are provided by distinct SPs. HIBC offers support to **Identity Federation** principle by specifying the *hierarchical storage* approach for identity storage and maintenance. In addition, HIBC model ensures **User Centricity** by incorporating numerous authentication protocols supported by distinct Cloud SPs and offers a *consistent user experience* to the service consumers. The HIBC model ensures **Privacy** through *limited disclosure* principle where same exclusive identity information is disclosed in each resource access request. However, no access control policies are specified in the model for ensuring the legitimate access by authoritative users hence lacks **Authorization** capability. Similarly, proposed HIBC model lacks **Auditing and Logging** capability.
   - ***Chord Based Identity Management for e-Healthcare Cloud Applications:*** Kim et al. (2010) presents an algorithm, Chord for Cloud (C4C) so that the customers of one Cloud may use the services of the other Cloud environments, with single user identity. Proposed C4C algorithm offers the

Authentication via *SSO* principle where session values are extracted from the user's service request and are verified by the SP (node). After successful verification, user is given access to the requested service thus offering user with seamless service provisioning. This algorithm offers support to **User Centricity** by incorporating protocols such as SAML and OpenID that ensures *consistent user experience*. Moreover, C4C follows the **Identity Federation** principle by offering the *distributed storage and computation* architecture. User credentials are disseminated among multiple Cloud nodes for authentication purposes, whereas sensitive identity information at each processing node is secured via Intrusion Detection Systems. In addition, C4C is composed of multiple components out of which Session Manager (SM) module is responsible for maintaining the information about valid user sessions and after successful verification, this SM module initiates the **Authorization** process. SM module creates session for each authenticated user and specifies valid time slot for each created session. To ensure **Privacy**, user credentials are kept encrypted throughout the valid user sessions and revoked after the session is terminated thus following *limited disclosure* principle. The algorithm does not does not support **Auditing and Logging** feature.

– ***Security APIs for My Private Cloud:*** A conceptual model along with the security architecture is presented in Chadwick and Casenove (2011) that describes a set of three security APIs each designed for a specific functionality. Authentication API deals with the verification and identification of users and sends back user's identity credentials to the Cloud. **Authentication** is provided via *SSO*, where user logouts are restricted to the Cloud applications only and session with the authentication IdP/server remains active. **Authorization** API on the basis of user's identity attributes and *access control policies* decides what rights a particular Cloud user may possess and when to revoke those access rights. These security APIs enable the Cloud users to protect their **Privacy** in Cloud by following *limited disclosure* principle where users can specify their own privacy policies for the protection of their information from other users. This model enables the Cloud resource owners to monitor and log the activities of their potential users, in order to ensure that only the legitimate resource can be accessed by the user having valid delegated attributes thus offers support to **Auditing and Logging** principle. In order to provide support to **User-Centricity**, proposed model offers support to multiple IdP protocols such as SAML and OpenID and offers *consistent user experience*. Moreover, this model enables the user to relate his identity information across multiple SPs to raise his assurance level for authentication purposes thus offering support to **Identity Federation** feature as well.

Functional behavior class

1. ***Anonymous IDMS***

   – ***An Identity-Based OTP Scheme with Anonymous Authentication:*** Identity based One-time Password (OTP) authentication scheme is presented in Luo et al. (2009) that operates on smart card based bilinear pairings. Proposed OTP scheme uses temporary identity information called *pseudonyms* to

ensure anonymity and **Privacy** by service consumers. Scheme utilizes smart card that is based on bilinear pairings and generates *OTP* along with the temporary user identity to ensure anonymity and security in the **Authentication** process. **Identity Federation** feature is ensured through the combination of smart card and OTP where identity information is collected from *multiple sources* to generate user credentials that are finally used in the process of authentication or **Authorization**. OTP scheme offers support to **User-Centricity** by incorporating *self-service* feature through password change facility module thus enabling the user to change or update his password without any assistance from the server side. However, the proposed OTP scheme offers no **Auditing and Logging** that maintains the logs of all user activities.

- ***UIMM Based on Anonymous Credentials*** Zhang and Chen (2010) proposes a Universal Identity Management Model (UIMM) where users are allowed to prove the ownership of their identity credentials without having to communicate with the IdP. In the proposed model, **Privacy** is ensured via *pseudonym* based signature scheme that ensures the minimal and selective disclosure of user information. The **Authentication** module includes IdP that provides the *identity credentials* to users and is also responsible for performing their verification. UIMM also ensures **Authorized** access to multiple federated security realms. The identity meta-system component aims to provide **User-Centricity** via identity selector component that allows the user to choose the credentials for different resource accesses. On the contrary, UIMM offers no support for **Identity Federation**; even though it allows the user to access the information from anywhere, but that information is retrieved from a central location, which may result in single point of failure. This model does not offer support to **Auditing and Logging** principle.
- ***An Entity-centric Approach for Privacy and Identity Management in Cloud Computing*** Angin et al. (2010) present an entity-centric architecture for Identity Management in Cloud that uses Active Bundles (AB) scheme and ensures user's anonymity by applying privacy preserving policies. Presented scheme offers **Privacy** via *limited disclosure* principle, which implements information disclosure policy provided by AB scheme. Identity data module of the AB scheme comprises of the encrypted authentication information that the SP requires while performing user **Authentication**. AB scheme incorporates a *Disclosure history* module that offers support to future information disclosure decisions considering past user interactions and ensure **Logging and Auditing** feature. However, proposed entity-centric architecture lacks support for **User-Centricity** since, no support for Consistent user experience is provided by the architecture. All the identity information is stored in the AB; a centralized location, **Identity Federation** principle is not followed. **Authorization** module that can ensure legitimate resource access is not incorporated in this architecture.

2. ***User-Centric IDMS***

   - ***Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing:*** Sánchez et al. (2012) presents a dynamic privacy-enhanced

federated identity management solution for on-demand resources provisioning in cloud computing scenarios. Proposed system provides **Privacy** management along with the complete control of users over their data through ECP and privacy engine modules. The system also offers **User Centricity** via user profile management module that allows the user to perform *self-service*. System incorporates **Authentication** module that supports various authentication mechanisms such as user *name/password* and *digital certificates*. User resource and service accesses are monitored via *activity monitoring* module, thus facilitating the **Auditing and Logging** feature. The **Authorization** module uses OAUTH protocol for the exchange of user's identity attributes in the process of authorization. Proposed system offers support to dynamic Cloud federation where Cloud trusts are established; however, it does not offer support to distributed storage mechanisms, hence, does not provide **Identity federation** features.

– ***User-Controlled Automated Identity Delegation:*** Hoellrigl et al. (2010) has described a user-controlled automated identity delegation solution that attempts to address the information consistency problem in a user-centric identity management system. Proposed system implements a User Access Management (UAM) module that enhances *OAUTH* protocol and offer support to **Authorization** via user defined *access control policies* and preferences. The system allows the user to *federate his identity* information across multiple IdPs thus offering support to **Identity Federation** feature. It offers **Authentication** by simple user *name and password* mechanism. It supports **User Centricity** by automating the process of disseminating the identity attributes in accordance with the user's *data disclosure preferences*. System fails to provide **Privacy**, since user information can be linked across various malicious SPs that may interact to correlate user identities. Similarly, this system does not monitor and log the user activities thus lack support to **Logging and Auditing** feature.

Discussion

Research findings & future research directions

We have performed an in-depth analysis of various Cloud based IDMSs in Section 'Results', which reveals that most of the systems do not offer support to all the essential features of Cloud IDMS and the ones that do, have their own weaknesses. None of the discussed techniques heuristically covers all the security features; moreover, they lack compliance to international standards which, understandably, undermines their credibility. Besides, identified features are worth considering, but are not mandatory as security and business requirements vary from one organization to the other. Organizations moving towards Cloud would benefit from this work by evaluating the security of the IDMSs in advance to avoid any adversity.

Furthermore, we have identified the current gaps, challenges and future key-trends related to Cloud identity management systems that must be considered by the Cloud identity service providers and subscribers. According to the most recent analysis, Identity with access management has been included among the top ten mega-trends for year 2014 by many well-known vendors and consultancy organizations including CA Technologies,

Gartner, Ping Identity and Oracle. Although the applications for managing identities vary from region to region, and even from business to business, they generally fall into one of the following areas.

1. ***Service automation:*** (Rose et al. 2011) By combining the individual's personal information into business processes organization shall be able to achieve efficient, automated and simplified transactions rather than the manual user input in activities such as user identification, authentication and authorization.
2. ***Increased user control:*** (Rose et al. 2011) Electronic identity enables the individuals to perform transactions on their own, without any assistance from the administrators or IT professionals. Self-service is a key example of user enablement. This aspect has recently achieved much attention from the IT industry and seems to continue its growth in new businesses as well.
3. ***Naming and identification of resources:*** Cloud providers offers wide range of services and resources including servers, storage and network to its subscribers. Therefore, to avoid any conflict and confusion, inter-Cloud IDMS must specify a mechanism for the naming and identification of Cloud services and resources.
4. ***Interoperability of Identity information:*** While performing user authentication and authorization, identity credentials could be expressed in a variety of ways for instance X.509 certificates, SAML assertions or WS-Federation security tokens. In inter-Cloud scenario, such representations result in syntactic and semantic issues hence requires interoperable identity information.
5. ***Identity life cycle Management:*** Throughout the life time of an entity, modifications in its attribute values, access permissions and service provisioning may occur. Consequently, all identity management systems are required to have updated and synchronized identity information to avoid any conflicts caused by the usage of old user data.
6. ***Single sign-on for interactions on the Inter-Cloud:*** Single sign-on must be implemented in a way that if users get successfully authenticated at one Cloud service provider, then throughput their valid session they must not be prompted again for authentication on any other (member) Cloud service provider.
7. ***Hardware components in cellular devices will become an increasingly important part of Identity management systems:*** (CA Technologies Predicts Key Trends for Identity and Access Management in 2014 (2014)) Due to the increase in the adoption of new mobile devices, advanced hardware protection technologies, such as ARM TrustZone, will become widely available. In addition to securing the hardware, users will be able to use their cell phones for authentication and identity proofing purposes while performing sensitive functions like financial transactions.
8. ***Lack of scalable identity proofing will continue to vex broader B2C/G2C deployments:*** As more and more users register for online services, validation of digital identities in an accurate and scalable manner is becoming a constant challenge (CA Technologies Predicts Key Trends for Identity and Access Management in 2014 (2014)). In addition to this, with the increase in identity proofing sources (such as new public and private records hosted by business or government organizations), the demand for scalable identity proofing will be further strengthened in 2014.

Consequently, it will require the IT industry to work in partnership and deliver scalable identity proofing mechanisms.

9. ***Risk-based authentication expands beyond Financial Services:*** The requirement for both strong authentication and consistent user experience will result in the widespread adoption of risk-based authentication systems. In such systems, the contextual information about service consumers, hardware devices and software applications is analyzed to determine the risk level for consumer's identity (CA Technologies Predicts Key Trends for Identity and Access Management in 2014 (2014)). Initially these services were adopted by the financial services only, however with the increase in requirement for improved security with improved user convenience; this technology will begin to be more widely adopted across other industries as well.

Above, we have provided a comprehensive list of state-of-the-art challenges and gaps that are needed to be addressed by the Cloud IDMS research community, and without which the very phenomenon of Cloud identity management is not fully achieved.

Conclusion

In this paper, we have presented research that is a step towards the development of an assessment criterion that can be used by other researchers and industry professionals to perform the evaluation of existing, as well as future Cloud based IDMSs. Since the domain of Cloud IDMS is still in its early stages, therefore, requires considerable attention from the research community and IT industry. We have contributed in this regard, by presenting a research work that holistically covers the domain of Cloud IDMSs. In particular, our contribution is multi-dimensional: first, we have presented a comprehensive list of security attacks that involve Cloud identity management systems and identity credentials as an attack tool or target, secondly we have identified the features that will act as countermeasure against the mentioned attacks. Thirdly, state-of-the-art mechanisms against each feature are filtered out with an objective to maximize their performance, security and interoperability. As another positive contribution, we have explicated the feature-mechanism relationship in the form of a well-organized taxonomy which is later used to analyze/evaluate various Cloud based IDMSs. Lastly, we have applied the previously discussed attacks against each Cloud IDMS to confirm their reliability and applicability in Cloud. Our findings from the analysis are presented in the subsequent tables which prove that Cloud IDMSs invariably have some pros and cons in their architecture and functionality. Furthermore, most of these Cloud IDMSs have limitations in terms of their reliability and applicability, as they are confined only to specific Cloud identity management scenarios. In conclusion, our work will augment the research which leads to the development and designing of a robust and holistically secure Cloud based IDMS covering all the identified features. Presented taxonomy will allow CSCs and CSPs to make a knowledgeable decision by selecting an appropriate IDMS that best satisfies their security and functional requirements.

Competing interests
The authors declare that they have no competing interests.

Authors' contributions
UH: has been lead author in drafting the manuscript, has conducted in-depth literature review, performed categorization, has done the detailed analysis of existing identity management solutions, and has revised the paper for important intellectual content. RM: has made key contributions to the paper conception and provided continuous support to the first author during all stages of the paper drafting,and gave final approval of the version to be published.

MAS: has significantly supported the first author during regular meetings, critically revised the paper for important intellectual content, provided new ideas, and gave final approval of the version to be published. MN: has significantly contributed to the research by introducing large-scale perspective for cloud IDMSs, critically revised the paper, and gave approval of the version to be published. All authors read and approved the final manuscript.

Acknowledgements
The authors would like to acknowledge the continual financial support provided by National University of Sciences and Technology (NUST) Pakistan in publishing related research papers. We would like to thank Ms. Yumna Ghazi for proofreading the paper.

Author details
[1]Department of Computing, School of Electrical Engineering & Computer Science, National University of Sciences & Technology (NUST), Sector H-12, Islamabad, Pakistan. [2]COMSATS Institute of IT, Islamabad, Pakistan.

Received: 19 July 2014 Accepted: 1 September 2014
Published online: 11 November 2014

References

Albeshri A, Caelli W: **Mutual protection in a cloud computing environment.** In *High Performance Computing and Communications (HPCC), 2010 12th IEEE International Conference on*. Piscataway, New Jersey, United States: IEEE; 2010:641-646.

Almorsy M, Grundy J, Müller I: **An analysis of the cloud computing security problem.** In *Proceedings of APSEC 2010 Cloud Workshop*. Sydney, Australia; 2010.

Alrodhan WA, Mitchell CJ: **Enhancing user authentication in claim-based identity management.** In *Collaborative Technologies and Systems (CTS), 2010 International Symposium on*. Piscataway, New Jersey, United States: IEEE; 2010:75–83.

Angin P, Bhargava B, Ranchal R, Singh N, Linderman M, Othmane LB, Lilien L: **An entity-centric approach for privacy and identity management in cloud computing.** In *Reliable Distributed Systems, 2010 29th IEEE Symposium on*. Piscataway, New Jersey, United States: IEEE; 2010:177–183.

Arias-Cabarcos P, Almenárez-Mendoza F, Marín-López A, Díaz-Sánchez D, Sánchez-Guerrero R: **A metric-based approach to assess risk for "on cloud" federated identity management.** *J Netw Syst Manag* 2012, **20:**513–533. Springer, 2012.

Ates M, Ravet S, Ahmat AM, Fayolle J: **An identity-centric internet: identity in the cloud, identity as a service and other delights.** In *2012 Seventh International Conference on Availability, Reliability and Security*. Piscataway, New Jersey, United States: IEEE; 2011:555–560.

Bertino E, Takahashi K: **IdentityManagement: Concepts, Technologies, and Systems:** ARTECH HOUSE, 16 Sussex Street, London SW1V 4RW UK; 2010.

Bhadauria R, Chaki R, Chaki N, Sanyal S: **A survey on security issues in cloud computing.** 2011. arXiv preprint arXiv:1109.5388.

Bhargav-Spantzel A, Camenisch J, Gross T, Sommer D: **User centricity: a taxonomy and open issues.** *J Comput Secur* 2007, **15:**493–527. IOS Press, 2007.

Brute Force Attack. *OWASP Testing Guide* 2013. [https://www.owasp.org/index.php/Brute_force_attack] [Online accessed September-2013].

CA Technologies Inc.: **CA Technologies Predicts Key Trends for Identity and Access Management in 2014.** 2014. [http://www.ca.com/us/news/press-releases/na/2014/ca-technologies-predicts-key-trends-for-identity-and-access-management-in-2014.aspx]. Online accessed April-2013.

Cameron K: *The laws of identity*: Microsoft Corp.; 2005.

Cao Y, Yang L: **A survey of identity management technology.** In *IEEE International Conference on Information Theory and Information Security (ICITIS)*: IEEE; 2010:287–293.

Celesti A, Tusa F, Villari M, Puliafito A: **Security and cloud computing: intercloud identity management infrastructure.** In *Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), 2010 19th IEEE International Workshop on*. Piscataway, New Jersey, United States: IEEE; 2010:263–265.

Chadwick DW, Casenove M: **Security APIs for my private cloud-granting access to anyone, from anywhere at any time.** In *Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on*. Piscataway, New Jersey, United States: IEEE; 2011:792–798.

Chang C-C: **Some forgery attacks on a remote user authentication scheme using smart cards.** *Informatica* 2003, **14:**289–294. IOS Press, 2003.

Chen D, Zhao H: **Data security and privacy protection issues in cloud computing.** In *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on. Volume 1*. Piscataway, New Jersey, United States: IEEE; 2012:647–651.

Chen J, Wu X, Zhang S, Zhang W, Niu Y: **A decentralized approach for implementing identity management in cloud computing.** In *Cloud and Green Computing (CGC), 2012 Second International Conference on*. Piscataway, New Jersey, United States: IEEE; 2012:770–776.

Chowdhury MM, Noll J: **Distributed identity for secure service interaction.** In *Wireless and Mobile Communications, 2007. ICWMC'07. Third International Conference on*. Piscataway, New Jersey, United States: IEEE; 2007:56.

Choudhury AJ, Kumar P, Sain M, Lim H, Jae-Lee H: **A strong user authentication framework for cloud computing.** In *Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific*. Piscataway, New Jersey, United States: IEEE; 2011:110–115.

Cloud Security Alliance: **Cloud Security Alliance SecaaS Guidance, Category 1: Identity and Access Management, 2012 by Cloud Security Alliance.** [https://cloudsecurityalliance.org/download/secaas-category-1-identity-and-access-management-implementation-guidance/] [Online accessed: November 2013], 2011.

Conrado C, Kamperman F, Schrijen GJ, Jonker W: **Privacy in an identity-based DRM system.** In *the Proceedings of Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on*. Piscataway, New Jersey, United States: IEEE; 2003:389–395.

Dhamija R, Dusseault L: **The seven flaws of identity management: usability and security challenges.** *IEEE Secur Privacy* 2008, **6:**24–29. IEEE, 2008.

Donevski A, Ristov S, Gusev M: **Security assessment of virtual machines in open source clouds.** In *Information & Communication Technology Electronics & Microelectronics (MIPRO), 2013 36th International Convention on*. Piscataway, New Jersey, United States: IEEE; 2013:1094–1099.

Eucalyptus Systems Inc.: **Eucalyptus Identity and Access Management (IAM).** 2012. [https://www.eucalyptus.com/docs/eucalyptus/4.0/security-guide/security_bp_access.html], [Online accessed August-2014].

Feng J, Chen Y, Ku WS, Liu P: **Analysis of integrity vulnerabilities and a non-repudiation protocol for cloud data storage platforms.** In *Parallel Processing Workshops (ICPPW), 2010 39th International Conference on*. Piscataway, New Jersey, United States: IEEE; 2010:251–258.

Ferdous MS, Poet R: **A comparative analysis of identity management systems.** In *High Performance Computing and Simulation (HPCS) 2012 International Conference on*. Piscataway, New Jersey, United States: IEEE; 2012:454–461.

Fox A, Griffith R, Joseph A, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I: *Above the Clouds: a Berkeley View of Cloud Computing*. Berkeley: Dept. Electrical Eng. and Comput. Sciences, University of California; 2009. Rep. UCB/EECS, 28, 13.

Gopalakrishnan A: **Cloud computing identity management.** *SETLabs Briefings* 2009, **7:**45–54.

Gunjan K, Sahoo G, Tiwari RK: **Identity management in cloud computing–a review.** In *International Journal of Engineering Research and Technology (Vol. 1, No. 4 (June-2012))*. Kudasan, Gandhinagar, Gujarat, India: ESRSA Publications; 2012.

Halpert B: *Auditing Cloud Computing: a Security and Privacy Guide (Vol. 21)*. Hoboken, New Jersey, USA: John Wiley & Sons; 2011.

Hoellrigl T, Kühner H, Dinger J, Hartenstein H: **User-controlled automated identity delegation.** In *Network and Service Management (CNSM), 2010 International Conference on*. Piscataway, New Jersey, United States: IEEE; 2010:230-233.

Jansen WA: **Cloud hooks: Security and privacy issues in cloud computing.** In *System Sciences (HICSS), 2011 44th Hawaii International Conference on*. Piscataway, New Jersey, United States: IEEE; 2011:1–10.

Jansen W, Grance T: *Guidelines on Security and Privacy in Public Cloud Computing*: NIST special publication, 800, 144, NIST; 2011.

Jensen M, Schwenk J, Gruschka N, Iacono LL: **On technical security issues in cloud computing.** In *Cloud Computing, 2009. CLOUD'09. IEEE International Conference on*. Piscataway, New Jersey, United States: IEEE; 2009:109–116.

Jøsang A, Fabre J, Hay B, Dalziel J, Pope S: **Trust requirements in identity management.** In *Proceedings of the 2005 Australasian workshop on Grid computing and e-research-Volume 44*: Australian Computer Society, Inc.; 2005:99–108.

Kim IK, Pervez Z, Khattak AM, Lee S: **Chord based identity management for e-Healthcare cloud applications.** In *Applications and the Internet (SAINT), 2010 10th IEEE/IPSJ International Symposium on*. Piscataway, New Jersey, United States: IEEE; 2010:391–394.

Kumar R, Gupta N, Charu S, Jain K, Jangir SK: *Open Source Solution for Cloud Computing Platform Using OpenStack*; 2014.

Kumaraswamy S, Lakshminarayanan S, Reiter M, Stein J, Wilson Y: **Domain 12: Guidance for Identity & Access Management V2. 1.** *Cloud Security Alliance* 2010. [https://cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf]

Lang U: **Openpmf scaas: authorization as a service for cloud & soa applications.** In *Cloud Computing Technology and Science (CloudCom) 2010 IEEE Second International Conference on*. Piscataway, New Jersey, United States: IEEE; 2010:634–643.

Leandro MA, Nascimento TJ, dos Santos DR, Westphall CM, Westphall CB: **Multi-tenancy authorization system with federated identity for cloud-based environments using shibboleth.** In *ICN 2012, The Eleventh International Conference on Networks*; 2012:88–93.

Leskinen J: **Evaluation criteria for future identity management.** In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*. Piscataway, New Jersey, United States: IEEE; 2012:801–806.

Li M, Yu S, Ren K, Lou W: **Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings.** In *Security and Privacy in Communication Networks*. Berlin, Heidelberg: Springer; 2010:89–106.

Luo S, Hu J, Chen Z: **An identity-based one-time password scheme with anonymous authentication.** In *Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC'09. International Conference on. Volume 2*. Piscataway, New Jersey, United States: IEEE; 2009:864–867.

Mahmood Z: **"Data location and security issues in cloud computing".** In *Emerging Intelligent Data and Web Technologies (EIDWT), 2011 International Conference on*. Piscataway, New Jersey, United States: IEEE; 2011:49–54.

Mather T, Kumaraswamy S, Latif S: *Cloud security and privacy: an enterprise perspective on risks and compliance*. Sebastopol, CA, USA: O'Reilly Media, Inc.; 2009.

McCallister E: *Guide to Protecting the Confidentiality of Personally Identifiable Information*. Collingdale, PA, United States: Diane Publishing; 2010.

Maler E, Mishra P, Philpott R: **Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML).** 2003. [https://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf]. Online accessed January-2013.

Meier JD, Farre C, Taylor J, Bansode P, Gregersen S, Sundararajan M, Boucher R: *Improving Web Services Security: Scenarios and Implementation Guidance for WCF*: Microsoft Developer Network; 2009.

Nabeel M, Bertino E, Kantarcioglu M, Thuraisingham B: **Towards privacy preserving access control in the cloud.** In *Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2011 7th International Conference on*. Piscataway, New Jersey, United States: IEEE; 2011:172–180.

O'Gorman L: **Comparing passwords, tokens, and biometrics for user authentication.** In *Proceedings of the IEEE. Volume 91(12)*. Piscataway, New Jersey, United States: IEEE; 2003:2021–2040.
Olden E: **Architecting a cloud-scale identity fabric.** *Computer* 2011, **44:**52–59. IEEE, 2011.
Pashalidis A, Mitchell CJ: **A taxonomy of single sign-on systems.** In *Information Security and Privacy*. Berlin, Heidelberg: Springer; 2003:249–264.
Pearson S, Benameur A: **Privacy, security and trust issues arising from cloud computing.** In *Cloud Computing Technology and Science (CloudCom) 2010 IEEE Second International Conference on*. Piscataway, New Jersey, United States: IEEE; 2010:693–702.
Ranchal R, Bhargava B, Othmane LB, Lilien L, Kim A, Kang M, Linderman M: **Protection of identity information in cloud computing without trusted third party.** In *Reliable Distributed Systems, 2010 29th IEEE Symposium on*. Piscataway, New Jersey, United States: IEEE; 2010:368–372.
Ratha NK, Connell JH, Bolle RM: **Enhancing security and privacy in biometrics-based authentication systems.** *IBM Syst J* 2001, **40:**614–634. IBM, 2001.
Rhoton J: **Discover OpenStack: the identity component keystone.** 2013. [http://www.ibm.com/developerworks/cloud/library/cl-openstack-keystone/index.html?ca=dat-]. Online accessed August 2014.
Rimal BP, Choi E, Lumb I: **A taxonomy and survey of cloud computing systems.** In *INC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on*. Piscataway, New Jersey, United States: IEEE; 2009:44–51.
Rose J, Rehse O, Rober B: *The value of our digital identity*: The Boston Consulting Group; 2011. [http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf], Online accessed March-2013.
Sanchez R, Almenares F, Arias P, Diaz-Sanchez D, Marín A: **Enhancing privacy and dynamic federation in IdM for consumer cloud computing.** *IEEE Trans Consum Electron* 2012, **58:**95–103. IEEE, 2012.
Salsano S, Veltri L, Papalilo D: **SIP security issues: the SIP authentication procedure and its processing load.** *Network* 2002, **16:**38–44. IEEE, 2002.
Saripalli P, Walters B: **Quirc: A quantitative impact and risk assessment framework for cloud security.** In *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*. Piscataway, New Jersey, United States: IEEE; 2010:280–288.
Saroiu S, Wolman A: **Enabling new mobile applications with location proofs.** In *Proceedings of the 10th workshop on Mobile Computing Systems and Applications*: ACM; 2009:3.
Senk C, Dotzler F: **Biometric Authentication as a service for enterprise identity management deployment: a data protection perspective.** In *Availability, Reliability and Security (ARES), 2011 Sixth International Conference on*. Piscataway, New Jersey, United States: IEEE; 2011:43–50.
Shin D, Lopes R, Claycomb W: **Authenticated dictionary-based attribute sharing in federated identity management.** In *Information Technology: New Generations, 2009. ITNG'09. Sixth International Conference on*. Piscataway, New Jersey, United States: IEEE; 2009:504–509.
Slone S: *Identity management. A white paper*: The open group identity management work area; 2004.
Sodhi G: **User provisioning with SPML.** *Inf Secur Tech Rep* 2004, **9**(1):86–96.
Subashini S, Kavitha V: **A survey on security issues in service delivery models of cloud computing.** *J Netw Comput Appl* 2011, **34:**1–11. Elsevier.
Suriadi S, Foo E, Jøsang A: **A user-centric federated single sign-on system.** *J Netw Comput Appl* 2009, **32:**388–401. Elsevier, 2009.
Thompson DR, Chaudhry N, Thompson CW: **"RFID security threat model".** In *the proceedings of Conference on Applied Research in Information Technology*; 2006.
Van der Hof S: *Innovating Government: An Introduction to the Book (pp. 1-14)*. R.J. Schimmelpennincklaan, JN Den Haag: TMC Asser Press; 2011.
Wang JJ, Mu S: **"Security issues and countermeasures in cloud computing".** In *Grey Systems and Intelligent Services (GSIS), 2011 IEEE International Conference on*. Piscataway, New Jersey, United States: IEEE; 2011:843–846.
Wang L, Wang L, Mambo M, Okamoto E: **New identity-based proxy re-encryption schemes to prevent collusion attacks.** In *Pairing-Based Cryptography-Pairing 2010*. Berlin, Heidelberg: Springer; 2010:327–346.
Windley PJ: *Digital Identity*. Sebastopol, CA, USA: O'Reilly Media, Inc.; 2005.
Yan L, Rong C, Zhao G: **Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography.** In *Cloud Computing*. Berlin, Heidelberg: Springer; 2009:167–177.
Yassin AA, Jin H, Ibrahim A, Qiang W, Zou D: **Efficient password-based two factors authentication in cloud computing.** *Int J Secur Appl* 2012, **6:**143–148.
You P, Peng Y, Liu W, Xue S: **Security issues and solutions in cloud computing.** In *Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on*. Piscataway, New Jersey, United States: IEEE; 2012:573–577.
Youseff L, Butrico M, Da Silva D: **Toward a unified ontology of cloud computing.** In *Grid Computing Environments Workshop, 2008. GCE'08*. Piscataway, New Jersey, United States: IEEE; 2008:1–10.
Zhang Y, Chen JL: **Universal identity management model based on anonymous credentials.** In *Services Computing (SCC), 2010 IEEE International Conference on*. Piscataway, New Jersey, United States: IEEE; 2010:305–312.
Zissis D, Lekkas D: **Addressing cloud computing security issues.** *Future Generat Comput Syst* 2012, **28:**583–592. Elsevier, 2012.
Zhou Y, Feng D: **Side-channel attacks: ten years after its publication and the impacts on cryptographic module security testing.** In *IACR Cryptology ePrint Archive, Volume 2005*; 2005:388.

doi:10.1186/s40294-014-0005-9
Cite this article as: Habiba *et al.*: Cloud identity management security issues & solutions: a taxonomy. *Complex Adaptive Systems Modeling* 2014 **2**:5.