ISSN 2278-3083

International Journal of Science and Applied Information Technology, Vol.7. No.1, Pages : 71-82 (2017)
Special Issue of ICSIC 2017 - Held during 23-24 September 2017 in Amman Arab University, Amman-Jordan
http://www.warse.org/IJSAIT/static/pdf/Issue/icsic2017sp12.pdf

Identity Management in cloud computing Challenges, threats and solutions

Kamal Ahmed Al Karaki [1], **Dr. Akram Al- Mashaykhi**[2]
[1]System Analyst, Jordan, kamal_karaki@yahoo.com
[2]Secretary General Assistant for research and studies , Jordan, akram.othman@gmail.com

Abstract

Identity Management in Cloud computing is one of the most important security challenges for managing and assuring a secure usage over multi-provider Inter-Cloud environments with dedicated communication infrastructures, security mechanisms, processes and policies.

Many researches on this subject were reviewed and found to be helpful in providing brief background on Identity Management in cloud computing and related issues. Some of these researches were theoretical (provided theory background basis about the subject). Others concentrated on the framework of research undertaken. But, the major pieces of work tackled methodology followed by previous researchers to introduce the main obstacles that hinder development of the sector and call for assistance.This paper describes the Identity Management challenges and threats and the available solutions .

Preface

In both traditional and artifact systems, the question of identity play a very important factor and role in protecting and securing the people, operations, resources, systems and information. Introduction

With possibility of remote access to information systems and other ICT infrastructure this issue becomes more important, and as information and its operation become a strategic and competitive factor for any aspects of modern life, this issue becomes more crucial.

Identity Management with open system environment with multi users each with multi way of access to the system and application in term of access tools vary from work station to PCs, laptops, I pads and other smart devices, with IT as a service Model and Virtualization of infrastructure, platform and software service through Cloud computation service and deployment models such new environment bring a new threats and challenges to security management in general and to identity control and management in particular.

Several attempts to address this problem were conducted by both the scientific research institutes and by leading ICT companies, these attempts provide different approaches and different tools with different efficiency and effectiveness measurements results and yet the subject open for farther effort for new and different and innovative methods, tools and product to cope with a very changing and demanding environment.

With the difficulties of controlling and managing the Identity based on the traditional and known methods and tools an increased demand for new different model to Identity management.

This work propose a model for Identity management stubble with specific set of requirements and constraints.

Significance of the Study

One of the big concerns of ICT community all over the world is the identity management, and its related activities.

The importance of this study came out from the importance of the problem of defining a framework for IdM suitable for open environment, in order to protect and secure the information assets which became a vital factor of modern economy and national security and individual privacy.

The Statement of the Problem

Sustainable accessibility to systems, applications, and other information assets and resources due to increased numbers of persons with different organizational levels and authorities for several and different purposes and needs, all through increased type of smart devices from multipoint of access and yet the situation still evolving and diversified.

Such state of affair of multi people may access from multipoint, and multi location by using multi devices for multipurpose in different time the information systems complicate the scene and bring the threats sustainable too, and make the control and management of identity in order to protect the most valuable assets of any organization in the globe more and more difficult.

problem may be stated as follows: still there are some limitations and shortfalls in the all current solutions for identity management in open distributed environment.

Concept and Background

Cloud Computing: Cloud computing phenomena and related conditions and environment have been under study by different scientists and researchers. Many pieces of research have been conducted to investigate such phenomena. A lot of papers were written on this subject. One of the main topics related to security of inter cloud is the identification of users and resources.

U.S. National Institute of Standards and Technology (NIST) defines cloud computing as :

"Cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”. (The NIST Definition of Cloud Computing. (Peter & Timothy, 2011). Figure (1) shows NIST Visual Model of Cloud Computing Definition.

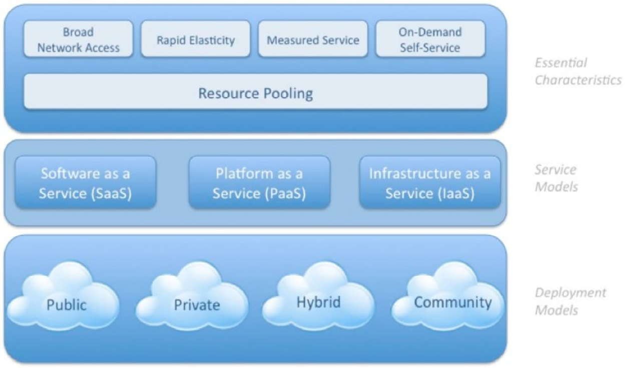

Figure (1): NIST Visual Model of Cloud Computing Definition

Cloud computation is based on Internet computation, where shared software, information and resources are offered to devices and computers on demand. It offers persons a way to share distributed services and resources that belong to various organizations. Since cloud computing is used the distribution of resources in an open environment, it is important to provide security and confidence for the exchange of data for development of cloud computing applications. This is an overview of cloud computing.

Identity management: On the internet, each user has multiple profiles and have write access for many different applications, provided by different service providers. This make many challenges to the service providers and users, in forms of security, synchronization of shared identities, etc. However, a strong need for a trusted genuine identity system across the internet and unambiguously identifying users and within enterprises. Federation of identities maintained by the multiple service providers on the cloud is very essential to the application integration and cloud based service composition. In this respect, an expected issue is the naming heterogeneity. Different factors used by different service providers for authentication such as email ID, PayPal ID, account number, etc.

Identity Management in Distributed environment has been recognized challenge. An example of this issue is the emergence of cloud computing, and specifically federated inter-clouds, only on a much larger scale and requiring more general solutions. several projects and groups identify the motivations, motivations, challenges and issues surrounding Federated Identity Management (Massimiliano et al., 2012) (Bernstein & Vij, 2010).

In traditional IT environment, service provision of Identity management is able to perform either through what possessed by user, characteristics, attributes that make up the identity of the real world to the user, through something assigned to the user by a third party entity or by something the derives from a user’s attainments and Passage. (Tewfiq & Jean, 2007) (Cao & Yang, 2010), this can be classified services required to facilitate identity management in these categories:

a. Identity style service, where the user is identified using trust records, history access records, reputation, and honor.

b. Identity service attribute, where the user is identified through specific attributes that are compatible with real-world entity

c. Identity ID service, where the user is identified through the allocation of specific identifiers, like e-mail or identity card number.

d. Identity accreditation service, where the user is identified through the adoption of a pre-set credentials like a digital certificates.

Literature Review

Cloud computing phenomena and related conditions and environment have been under study by different scientists and researchers. Many pieces of research have been conducted to investigate such phenomena. A lot of papers were written on this subject. In the following paragraphs a summary briefing the literature review is provided.

Roshni & et al. 2013, studied cloud computation as a new trend of computation concept that presents a scalable resources on demand. It is being under attacks and have risk for data confidentiality. The researchers reviewed different identity management frames that proved to be helpful in making cloud environment more safe.

The main remarks of this study writers were:

1) Identity Management System provides the management with multiple digital identities. And decides how to reveal individually particular information (PII) of entities to obtain exact service.
2) IDM does the following tasks:
   a) Set up identities: comparing individually particular information with a user.
   b) Describe identities: delegate attribute identifying a user.
   c) Record the uses of identity data: store the personality movement in a system.
   d) Destroy an identity: after the completion of the work personally identifiable information of the user become unusable.
3) Identity Management use one of these categories of identifiers:

a. Identifiers that both a user and Service Provider know.
b. Identifiers known by Providers may verify via these providers.
c. Identifiers that an entity is unique markers(on example retina).

Juraj & et al. 2009, pointed out the main problems facing cloud computation as follows :

1) Services as Facebook, MySpace and YouTube are more or less well-known to everybody, of course there is Google, which launches new services all the time. However, this vast amount of services create a problem, Internet users have to be active to remember the many pairs of user name/password of these different services.
2) As of security outlook, main problem in OpenID seems to be its weakness in the application.

The major results of the paper were as follows:

1) Majority of the applications need information concerning users than just an identifiers.
2) Such information may be generated either by users who input the values or from attributes received through authentication.
3) Storing these values locally creates duplication of the information and pushes users to maintain them manually.
4) OpenID has obtained amounts of popularity. With popular service suppliers starting supporting it, it became popular. However It is strength (being open) has became its limitation.
5) If service needs any additional information, it may generate that from user, confirm it, when it is necessary, and store it locally.
6) Protocol’s weakness for phishing is also an issue to be studied and solved.

Audun & et al. in 2007, summarized the major problems facing cloud computing as follows:

1) The quick growth in the number of online facilities that leads to increasing numbers of various identities needed by every user to manage.
2) Lots of people feel overloaded with identities and badly affected from password exhaustion, a problem that makes people unable appropriately control and protect their digital identities against identities theft.
3) Lots of identity management systems are planned to be scalable and cost effective from the view of the service provider (indicated Service Provider in future), which sometime create poor usability and inconvenience from the users' perception.
4) Being Service Provider centric, traditional identity management systems have largely overlooked the fact that very frequently, equally important for users to be able to authenticate Service Providers, the same for Service Providers to authenticate users.

The paper proposed a general approach to make users better and be able to control and manage their identities, as well as in the creation of more secure identity management solutions. In particular, a user-centric approach based on hardware and software technology on the user-side, aims at helping users accessing online services.

Amir & Thomas in 2005, proposed a Framework for an Interoperable Electronic Identity Management System, considering that electronic identity (eID) tokens have been rolled out to the citizens of several member states in the European Union (EU). Giving a method of Identification, Authentication and electronic Signatures (IAS) to individuals for online transactions is the primary aim of these eID tokens. Member States made heavy investments to build the e-government and the infrastructure services to support eID tokens. Meanwhile, the electronic identity management systems of Member States lack the wanted interoperability aspect. After studying the current system, the researchers proposed a simple solution to solve some of the major interoperability problems.

The paper suggested a framework that provides an interoperable solution that could be accepted publicly if it met some simple conditions. The solution must be able to grant advanced security but not compromise the privacy of citizens.

The paper considered eID tokens to be the upcoming linking tools between citizens and public sector and concluded by saying that they are being issued to citizens across Europe by Governments. The framework provided solid steps to secure citizen’s privacy while granting better security.

Unauthorized Access in the Cloud Computing Environment was detected by Rasim & Fargana in 2014, so they proposed a method to expose unauthorized access to the cloud infrastructure. Collaborative Filtering Algorithm constructed on the cloud model was used to build the process. By modeling the ordinary actions of cloud users in the form of a cloud models, and comparing them with each other by utilizing the cosine similarity method. After using the collaborative filtering method, the deviations from the normal behavior are evaluated. If the deviation values are higher than the set limit, the user who was permitted to the system is evaluated as illegal, if not, he is evaluated as a real user.

The paper, proposed a collaborative filtering algorithm built upon the cloud model to be utilized to detect the masquerade attacks in the cloud infrastructure.

The paper pointed out that the model could aid in identifying similarities between the users on the basis of the cloud model. While utilizing the similarity measurement method based on the cloud model, it doesn't demand a strict comparison between different users' score value of operations.

Identity Management Challenges, threats and available solutions

Cloud computation Challenge and threats:

Cloud computation consists of three parties: Cloud user (Customer), Cloud Network and cloud Service Provider (CSP). And many security challenges faced at different levels and threats, like challenges and threats at user/host level, network Level and Cloud Service Provider level. These challenges and threats must be dealt with since it is necessary to keep the cloud up and running continuously (Umme et al., 2014):

Table (1): Identity Management Challenge and threats

Challenge	Description	Threats
1) Intercloud resources Identification and Naming	Surplus types of shared resources in the cloud computation model puts the infrastructure of cloud computation users want to make sure the identity of the request resources as it should know for sure who is the one resource they want to ask.	**1.** Univocality of resources' identity and unambiguous requests. **2.** Problem of Continuous need for updating of documents
2) Identity information Interoperability in the Intercloud	Outsourcing internal services is a major reason for the enterprise to use the cloud computation model. Some organizations like to adopt this model because of the cost effective they practice while they go through out sourcing. The services and applications inside a company are not separate, and usually they form a network of dependencies, with compound relation between them; few of this services may not be outsourced. Then it should be given special attention on Interoperability.	**1.** Use of language **2.** The interoperability problems (Syntactic and Semantic obstacles) **3.** Limitation of initiatives **4.** Common services related with identity management
3) Inter-cloud's life cycle identity management	During the life cycle of an entity's digital identity, various changes concerning provision, attributes, entitlement, or authorization may be happened depending on an organization's policy and entity's behavior or availability. A quick Synchronization of these changes, to all involves parties inside the Intercloud, appears to be imperative to assure that every entity has the same confrontation.	**1.** Synchronization delays
4) Interactions of Single sign-on in the Intercloud	With Intercloud increase the numbers of potential interactions that can happened between the various users involved in the data. In such interactions, the parties concerned to exchange identity information, authentication and identification purposes in spite of the existence of preceding knowledge of each others own identity information or not.	❖ **Threats for Cloud Service Users** **1.** Ambiguous responsibility **2.** Loss of judgment **3.** Lost of confidence **4.** Service Provider Lock-in **5.** Unsecure User Access of Cloud Service **6.** Deficiency of information/Asset Management **7.** Data leakages and lost **Threats for Cloud Service Providers** **1.** Ambiguous responsibility **2.** Protection Contradiction **3.** Evolution Risks **4.** Business Interruption **5.** Supplier Lock-in **6.** License Risks **7.** Regulation Conflicts **8.** Shared Environment **9.** Unsecure Administration (API) **10.** Bad Integration **11.** Hypervisor Isolation Failure **12.** Service Unavailability **13.** Data Unreliability **14.** Abuse of the Rights of Cloud Service Providers

Solutions available to meet the challenges and threats IDM

Available solutions to the challenges IDM and threats shown in Table (2) are:

a) Intercloud resources Identification and Naming

The existing approach for identifying and naming Cloud resources was shown in (Celesti et al., 2010), on base on the use of Extensible Resource Identifier (XRI, 2015) and eXtensible Resource Descriptor Sequence" (XRDS, 2015). XRI is a resolution and scheme protocol for abstract identifiers in harmony with uniform resource identifiers (URI) (In computation, a uniform resource identifier is a set of Characters used to identify the resources names). This selection can affect the representation of resources on the network. While XRDS is an XML-based general layout for service discovery and resource description, XRDS enable the resources description, in addition to, their related services, these are named service endpoints (SEPs).

Interoperability of identity information in the Intercloud

With respect to issues of compatibility between different themes on the semantic level plans and standards such as ITU-T Recommendation X520 (X.520, 2008) and ITU-T Recommendation X521 (X.521, 2008), (Recommendation X520 defines a number of attributes types and matching rules that might be helpful for a variety of applications to lead single particular use for many of the specific features in the names formation, particularly for categories of objects specified in Recommendation ITU-T X521. There are other types of attributes and qualities and called on the notification, and provide diagnostic information that recommendation, identifies the international standards connection types that supply associated with the attribute values of properties, also includes definitions of sentences LDAP relevant to attribute types and rules of matching). and references 4519 (Request for Comments) 4524 and (Sciberras, 2006) (Zeilenga, 2006).

These initiatives are not enough in Intercloud; There is need for solutions that have additional kinds of services, resources, and subjects. The use of ontologies can tackle problems of interoperability (Wache et al., 2001) (Priebe, et al., 2006), that might make integration of heterogeneous attribute schemes possible.

b) Inter-cloud’s life cycle identity management

In this direction, Service Provisioning Markup Language (SPML) proposed by OASIS, an XML framework for managing allocation and Provisioning of system resources and identity information inside and between organizations (SPML, 2003).

SPML Version-1 was built on the OASIS Directory Services Markup Language (DSML, 2015) Version-2 (an XML representation of the Lightweight Directory Access Protocol), it is expected to join a family of standards designed to ease the implementation of Web services, and to establish interoperability surrounded by provisioning systems that allow organizations to securely create end-user accounts for applications and Web services from a single point in an organization.

One SPML request message may be used to create user accounts at the same time in a multi-provisioning systems. De-provisioning is done by closing access accounts for any employee leave a company. This excludes dead accounts and prevents ex-employees from gaining access to customer systems.

c) Interactions of Single sign-on in the Intercloud

In this direction, proposing an infrastructure for identity management capable of supporting authentication between the Federal clouds, based on the assertions SAML, in **(** Tusa et al., 2010) and Openid can solve this problem. Openid and SAML were discussed in next topic.

Table (2): Available solutions for challenges and threats

challenge	description	**Name of Products**
Intercloud resources Identification and Naming	It is essential that each service is described independently, but this is not the case in the Intercloud environment.	• XRI • XRDS • XRD 1.0
Interoperability of identity information in the Intercloud	Traditional identity management systems Interoperability problems appears in the Intercloud.	• X.521 and X.520 ITU-T Recommendations • RFCs 4519 and 4524 (Request for Comments)
Inter-cloud’s life cycle identity management	A quick Synchronization of changes happened during the life cycle of an entity’s digital identity concerning provision, attributes, entitlement, or authorization, to all involves parties inside the Intercloud, appears to be imperative to assure that every entity has the same confrontation	• Service Provisioning Markup Language (SPML)
Interactions of Single sign-on in the Intercloud	The parties concerned with exchange identity information, authentication and identification purposes in spite of the existence of preceding knowledge of each other's own identity information or not.	• SAML • OpenID

State of the art of Solutions Approaches

This section present brief description for the Identity Management frameworks:

Framework definition

A Framework is a conceptual or real structure created to act as a guide or support to create something that changes the structure to be useful. A framework is usually more prescriptive than a structure and more comprehensive than a protocol.

Identity management frameworks

There are many Identity Management Frameworks as:

1. Security Assertion Markup Language (SAML)

It is an open standard data format for exchange of authentication and authorization data between identity Provider and Service Provider via internet. (Lewis & Lewis, 2009). The Consortium for defining SAML standard and security is Organization for the Advancement of Structured Information Standards (OASIS) (Juraj et al., 2012) . There are three versions of SAML: SAML1.0, SAML1.1 and the new major version of SAML is 2.0 became an official OASIS standard in March 2005.

The four Components of SAML are: (Juraj et al., 2012)

1. Assertions: SAML assertion is the transaction from the identity Provider to the Service Provider.
2. Protocols: Which are used to communicate assertions between the service provider and identity Provider.
3. Bindings: Which are used to Map the SAML Protocol on to lower level network communication Protocols which are used to transport the SAML assertion between the identity Provider and Service Provider.
4. Profiles: The highest level of SAML Component which use cases between identity Provider and Service Provider that indicate how assertion, Protocols and Bindings will work together to Provide single-sign-on.

The Identity Provider or the Service Provider can initiate the web browser Single-sign-on profile. If the Identity Provider initiates it, the assertion is either encrypted, signed, or both. Figure (2) shows the Identity Provider Initiated SAML, assertion Flowchart.

SAML is a single login process so that you only log in once using your username and password and use many services and applications at once. So, the time spent by users to log into multiple platforms and applications is reduced. SAML also improves the effectiveness of all Networks. It also reduces the Administrative expenses. SAML does not require user information to be maintained and synchronized between databases. The limitations of SAML are single point of failure. It adds the cost and the necessary information disclosure between the trusting site and SSO authority.

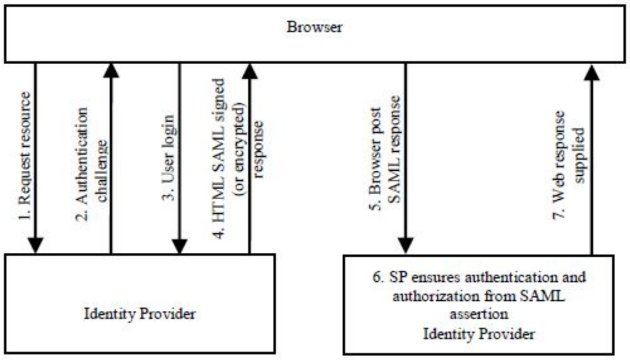
Browser
1. Request resource
2. Authentication challenge
3. User login
4. HTML SAML signed (or encrypted) response
5. Browser post SAML response
7. Web response supplied
Identity Provider
6. SP ensures authentication and authorization from SAML assertion
Identity Provider

Figure (2): Identity Provider Initiated SAML Assertion Flowchart

(Somorovsky et al., 2012)

2. Liberty Alliance

Liberty Alliance defines sets of protocols which collectively offer solutions for identity federation management, cross-domain authentication and session management (Scott et al., 2004). Liberty Alliance Circle includes User, Service Provider (SP), and Identity Provider (IdP). It is the single-sign-on in which no need to authenticate again. Steps for single-sign-on being as given in figure (3)

While the identity is proven by Authentication, another concept is used called Authorization. Authorization is used to grant access permissions for users with multiple levels. After finishing the Authentication, Authorization and Single Sign-On mechanism, Liberty Alliance specifications also include the Single Sign-Out mechanism.

The user sends request for single Logout to identity Provider. Identity Provider directing the request to Service Provider. Service Provider does Process for Log out. Service Provider sends response to the Identity Provider. Identity Provider forward Single Log out confirmed to the user. The Liberty Alliance is Single-Sign-On and it authenticate and Authorize user Profiles. It also Provide the Scalability (Dwiputera & Ruppa, 2012).

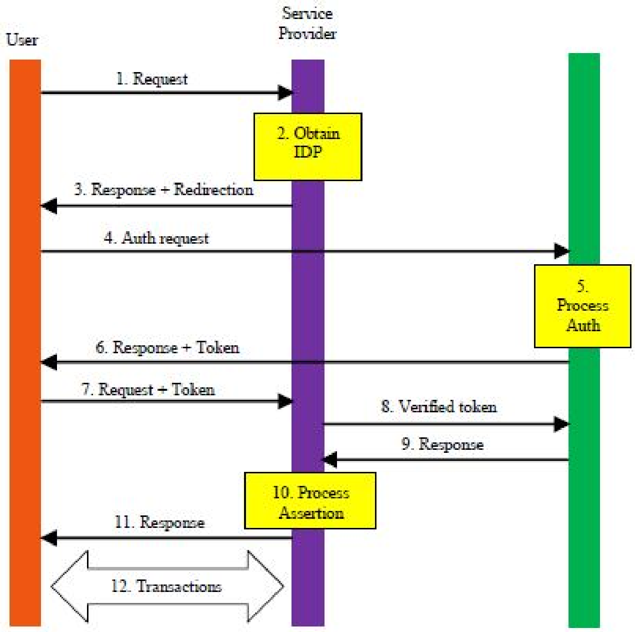

Figure (3): Single-Sign-On
(Dwiputera & Ruppa, 2012)

3. Windows CardSpace

Windows CardSpace is an Identity metasystem (system of systems) that gives a method, to manage a user's multi digital identities (Bhargava et al., 2011). It depends on the Concept of an Information Card based access platform/ architecture, developed for windows XP. A plug-in for Internet explorer 7 browser is used. Microsoft CardSpace is based on Web Service-Federation protocol which consists of the following specifications giving a base model for federation between Relying Parties and Identity Providers: WS-Security, WS-Security Policy, WS-Trust. Three parties are involved in this identity system:

1) Identity providers: Which supply digital identities (as trusted third-party).

2) Relying Parties: Identities are required to offer a services to users

3) Service requestor: Individuals and other entities related to whom claims are made.

The CardSpace identity metasystem makes use of XML based protocols, impeding the Simple Object Access Protocol (SOAP) and Web Services protocols). The message flows of the CardSpace framework are as in figure (4).

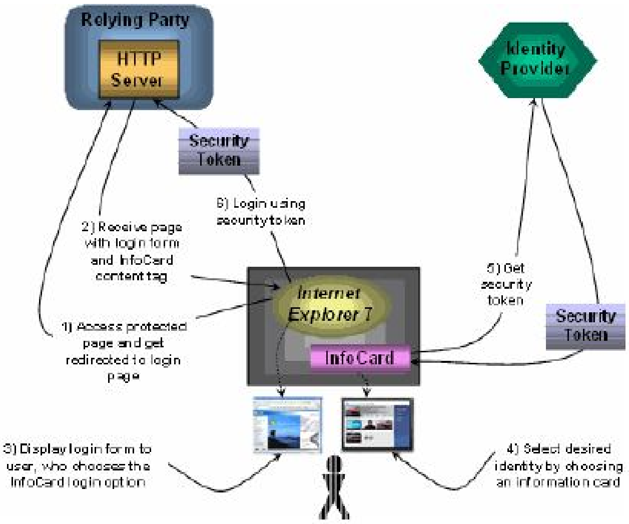
Relying Party
HTTP Server
Security Token
Identity Provider
6) Login using security token
2) Receive page with login form and InfoCard content tag
5) Get security token
Internet Explorer 7
Security Token
1) Access protected page and get redirected to login page
InfoCard
3) Display login form to user, who chooses the InfoCard login option
4) Select desired identity by choosing an information card

Figure (4): CardSpace Model of Identity Management
(Bhargava et al., 2011)

It is more flexible than user name and password. It employs strong cryptography, making it safer than password for use. It can potentially support any type of identity claim that it makes sense to all of the interacting parties and that users are ready to release. The CardSpace framework is criticized due to its reliance on the user's judgment of the confidence of an Relying Party. Many of them do not pay attention when asked to approve a digital certificate of an Relying Party, either because they know that they must approve the certificate in order to get access to a particular website or because they do not know the importance of the approval decision. Relying Parties with no certificate may be used in the CardSpace framework. In a case where multiple Relying Parties and one Identity Provider are involved in a working session, the security identity meta system inside the session will depend on the authentication of the user to the Identity Provider only. In the case of the password is cracked or a working session is snatched the security of the entire system is threatened. To defeat the security imitation mentioned above use the Zero-Knowledge Proofing, Selective Disclosure, Anonymous Credential (Bhargava et al., 2011).

4. Privacy and Identity Management for Europe (PRIME)

PRIME is a project for privacy architecture production, and a model and various application Scenarios (Camenisch et al., 2005). The three parties involved in PRIME are: User, Service Provider and Certification Authority. User requests for services or resources to service provider, and Service Provider provide the services as per user demand. Certification Authority is certifying authority (special type of service provider), which issued the certificates that are digitally signed statement. The PRIME involves four cryptographic tools namely secure communication, anonymous communication, pseudonyms, credentials and proofs of credentials ownership. Figure (5) present the execution of transactions.

PRIME is an User-controlled privacy-enhancing means that each individual user is put into control with respect to her/his Personally identifiable information (PII) as possible. It is comprehensive means bringing diverse research areas (system architecture, cryptography, policies) and models together such as Designing and evaluating early models, learn some lessons how to integrate their achievements, and close the remaining gaps. It is a large scale means that system architecture, privacy and security mechanisms, terminology, prototypes, and tutorials are developed, evaluated and presented to the public. **The Limitations of PRIME is that the product is not standardized and it is only possible unless it is interoperable with existing systems. It has its middleware which should be implemented on senders and receiver side console, which is an extra overhead** (Camenisch et al., 2005).

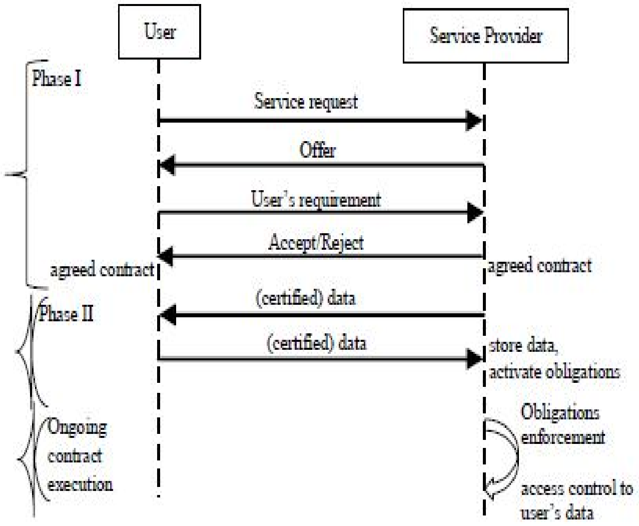

Figure (5): Execution of a transaction (Camenisch et al., 2005)

5. OpenID

OpenID is an easier way, faster, and safer way to log on to websites. OpenID is a no centralized model for identity management, that permits service providers to delegate the users authentication to identity provider. In this model, the user identity is represented by a Uniform Resource Locator (URL), called an OpenID identifier. Thus, users do not need to do an account for each site; but, they just use their OpenID identifier, and the authentication procedure will be conducted through the user's identity provider (David et al., 2012).

The limitations of OpenId are Phishing Attacks.

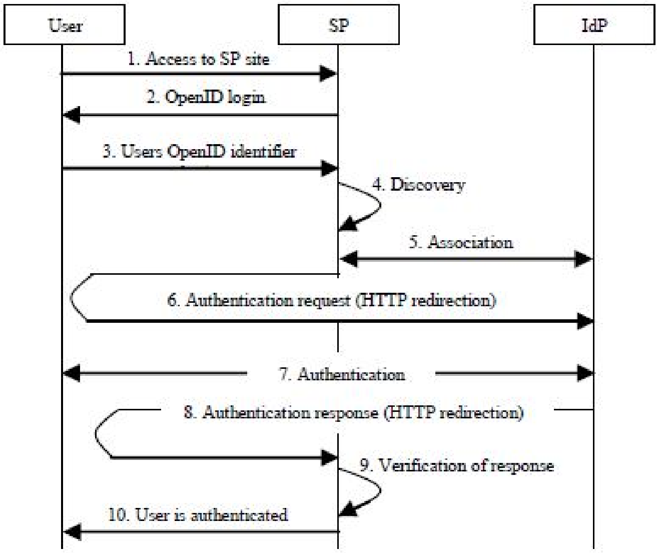
User
SP
IdP
1. Access to SP site
2. OpenID login
3. Users OpenID identifier
4. Discovery
5. Association
6. Authentication request (HTTP redirection)
7. Authentication
8. Authentication response (HTTP redirection)
9. Verification of response
10. User is authenticated

Figure (6): OpenID Authentication protocol (David et al., 2012)

6. OAuth

OAuth is an Open Authentication method where user can share his stored resources to specific site with any other site instead of having to hand out her/his username and password (OAuth, 2007). It is flexible and designed to work with mobile devices and desktop applications. OAuth use Digital Signature, Hash Algorithm, Shared Secret, Nonce, Time Stamp. If the OAuth standard is extended by info cards support or other functionality in the future, it may be easily supported in any application. It is easy to manage or maintain configure to them. for example extranet login models with mixed authentication like SAML. It is Less data to store on servers.

7. OneLogin

OneLogin is the Single-Sign-On and Identity management for Cloud based Applications. It is good web applications for Saas. It is used to improve SaaS applications security, having a Centralized Password, user can get many secure password among his network of applications because he cannot remember all of them. OneLogin works by installing a browser extension that effectively pastes the credentials into the applications and logs user in. It supports the main Browser such as Chrome Firefox, Safari, and also supports the main windows OS's, Linux, Macintosh. Lightweight Directory Access Protocol and Active Directory , are available. It also supplies the De-Provisioning. OneLogin's Cloud identity platform comes ready for secure single sign-on for mobile, iPad and web, federated search, user provisioning, deep directory integration with real-time user sync, out of band multiple factor authentication, A virtual private network integration and compliance reporting. OneLogin's catalog contains many thousands of pre-integrated applications, like Oracle CRM On-Demand, Salesforce.com, Microsoft Office 365, Google Apps, NetSuite, Innotas, LotusLive, Success Factors, WebEx, Workday, Yammer, Service Now (OneLogin, 2010).The Advantages of OneLogin are :

1) Beautiful User experience
2) Simple to set up
3) Easy to use
4) Cross Platform and Cross Browser Support
5) Two factors authentication are available,
6) It is possible to add customer applications and any new applications.

Limitations of OneLogin are (OneLogin, 2010):

1) An application level only.
2) De-provisioning just prevent access to onelogin, don't lock or delete the application.
3) Don't do role on base on security.

8. Windows Identity Foundation (WIF)

It is a Microsoft software framework for construction identity awake application. It is a framework for implementing claims on bases of identity in applications. The web services that use Windows Identity Foundation, the .NET frame work version 3.5 service provider (WIF, 2015) The Characteristics of Windows Identity Foundation are as follows:

1) It provides templates which building claim-aware application.
2) It includes functionality that lets identities to be maintained across multiple service boundaries.
3) It includes a utility which help developers translate between NT tokens and claims.
4) It let developer to build claim-aware application by provide APIs.
5) It provides tools that helps developers to build custom security token services using ASP.NET.
6) It provide a ASP.NET controls which help developers to create web pages in claims-aware applications.
7) It provides utilities that create a trust relationship between a Security Token Service and Relying Party application.

The Claim-based identity involves Claim, Security Token, Security Token Service and Relying Party. Claim is identity information like email address, name, age. In Security Token the user delivers a set of claims together with his request. In a Web service, this claims are carried in the security header of the SOAP packet. In a browser-based Web application, the claims arrive via an HTTP POST from the user's browser, and may later be cached in a cookie if a session is desired. They have to be serialized somehow, and this is where security tokens come in. It is a serialized set of claims that is digitally signed by the issuing authority. In security token service it is the plumbing that builds, signs, and issues security tokens according to the interoperability protocols. In Relying Party when you build an application that relies on claims.

3.5 Review of identity management framework in cloud

Table (3)(a) and table(3)(b) presents Identity Management Frameworks and it's Attributes and it contains comparison of different identity frameworks. It shows that all of them depends on Relying party/service provider initiated and there are limitations for some frameworks. It also suggests that in some of the identity frameworks, the registration and identity provider initiation are not required. Although most of the frameworks support single-sign-on, earlier identity frameworks were adopted by e-mail providers and corporate organizations use and government; currently they are extensively used in social networking sites and mobile apps.

Table (3)(a): Identity Management Frameworks & it's Attributes (Roshni et al., 2013)

Identity Framework	**SAML**	**Liberty Alliance**	**Windows Cardspace**	**PRIME**
Registration required?	NO	Yes	Manifested through the installation of managed cards into the selection	Restricted to registered user
Protocols Used	SAM, XML, SOAP, HTTP	LDAP, XML	XML based	Cryptographic protocols
limitations	The limitations of SAML are single point of failure. It added the cost and also the necessary information disclosure between the trusting site and SSO authority	N/A	Major limitation of the Window Cardspace is relying on single layer authentication and second is relying on the third party Another drawback is the judgment of the user in trusting the RP certificate and sometimes, in the CardSpace framework RPs with no certificates at all are used.	A major limitation of PRIME is that it requires user agents and service providers to implement the PRIME middleware
Identity provider initiated	Yes	Yes	NO	Yes
Main Purpose	Single-sign-on for enterprise users	Create an open network identity infrastructure	Single-sign-on for websites	For Data Minimization

Table (3)(b): Identity Management Frameworks & it's Attributes (Roshni et al., 2013)

Identity Framework	**OPENID**	**OAUTH**	**OneLogin**	**Windows Identity Foundation**
Registration required?	NO	Explicit identity services pre-register for a consumer key & secret	Yes	Yes
Protocols Used	XRDS, HTTP	JSON,HTTP	RDF,X.509	WS-Trust, WS-Security, WS-Federation
limitations	highly at risk of phishing attacks.	N/A	N/A	N/A
Identity provider initiated	NO	Expected for OAUTH V2.0	Yes	Yes
Main Purpose	Single-sign-on for Consumers	API authentication between applications	Single-Sign-On for Companies to secure access web application	Tempering/Disclosure of Credential or other Sensitive data

Conclusion and Recommendations

Conclusion

In this paper, the researcher has highlighted the major issues for identity management in open environments as cloud environment and inter cloud environment through the presentation of the their definitions and major related subjects. It illustrates challenges and threats for cloud computation and intercloud environment challenges and available solutions.

General findings of the paper maybe summarized as follows :

1. Number of users and resources for internet and inter cloud are increasing over time.

2. Security is critical issue to the intercloud environment, a fact that should be undertaken into consideration and put under focus during all stages since we are not just dealing with financial transactions that can be tackled through penalties in case there is a data breach. Here we are talking about systems with infiltration that could lead to loss of lives and/or cause massive disturbance to the society.

3. Privacy and security remain a high level threat in the management environment of cloud data, taking into account that the data's privacy is influenced as the users of cloud don't have full awareness about the data's location in servers.

Identity Management Findings

1. Users of cloud services can only access using the deployed services to access, modify, and remove their information, that are out sourced by them (whatever the private or public data) and these can only be accessed using deployed services.

2. Identity management issue is very important for the environment of cloud computing. The management of user credentials and remote access introduced concerns for privacy. Many ways to deal with the issue exist, but a few of those offered a simple and trust-based method for the service and application of cloud computing.

3. Most of previous solutions for identity management in intercloud environments still have limitations and shortfalls

Recommendations

Based on the above, the following should be kept in mind regarding cloud computing, management and security:

1) Implies a better method to enhance the abilities substantially with no expenses spent in new infrastructure or licensing new software.
2) Despite the efficient use of resources by virtualization techniques and taking up a lot of the work load from the user, security risks fraught cloud computing, and this issued should be highly considered.
3) Usual identity management systems are designed to be cost effective and scalable mainly for the SPs, but not essentially for the users, and that often causes poor usability.

4) Pear in mind that any framework will have some limitations, it is expected that extensive future research will be of value as it may cover any gap areas in this regard.
5) Further research is appreciated and encouraged in particular fields such as identity management for open distributed environment.

At the end of this paper, the research has the hope that the current paper will help in covering a gap that is may existed and provoke problems to researchers in the subject. Further research is appreciated and encouraged in particular fields such as identity management for open distributed environment.

References

1. Amir, H., and Thomas, R. (2005). **Proposed Framework for an interoperable electronic IdM**. (Gartner. Gartner survey on consumer trust in online commerce 06/2005)
2. Audun, J., Mohammed, A. and Suriadi, S. (2007). **Usability and Privacy in Identity Management Architectures**, In the Australasian Information Security Workshop: Privacy Enhancing Technologies (AISW 2007).
3. Bernstein, D., and Vij, D. (2010). **Intercloud Security Considerations**, *2nd IEEE International conference on Cloud Computing Technology and Science*, pp. 537–544 (2010).
4. Bhargava, B., Singh, N., and Sinclair, A., (2011). **Privacy in Cloud Computing Through Identity Management**. Technical Report. Computer Science, Purdue University.
5. Camenisch, J., Shelat, A., Sommer, D., Fischer, S., Hansen, M., Krasemann, H., Lacoste, G., Leenes, R., and Tseng, J. (2005). **Privacy and identity management for everyone**. In Proceedings of the Workshop on Digital Identity Management.
6. Cao, Y., and Yang, L. (2010). **A Survey of Identity Management Technology**. In Information Theory and Information Security (ICITIS), 2010 IEEE International Conference On, 287-293.
7. Celesti, A., Villari, M., Puliafito, A. (2010). **A naming system applied to a RESERVOIR cloud**. Sixth International Conference on Information Assurance and Security (2010).
8. David, N., Isaac, A., Prokopios, D., and Stefanos, G. (2011**). Identity Management Challenges for Intercloud Applications**, 1st International Workshop on Security and Trust for Applications in Virtualised Environments (STAVE 2011).
9. DSML (2015). **Directory Services Markup Language**, retrieved from http://searchoracle.techtarget.com/definition/DSML
10. Dwiputera, F., and Ruppa, S. (2012). **Single sign-on architecture in public networks (Liberty Alliance).** In Proceedings of the INFOTECH seminar on advanced communication Services (ACS).
11. Juraj, S., Mayer, A., Worth, A., Schwenk , J., Kampmann, M., and Kari, H. (2009). **OpenID and identity management in consumer services on the Internet**, TKK T-110.5190 Seminar on Internetworking 2009-04-27, Helsinki University of Technology.
12. Lewis, K., and Lewis, J. (2009). **Web single sign-on authentication using SAML**, International Journal of Computer Science Issues, 2009, Vol. 2, pp. 41-48
13. Massimiliano, R., Hamza, G., Massimo, F., Neeraj, S., Jesus, L., Silviu, P., and Dana, P. (2012**). Security Issues in Cloud Federations, Chapter 10 in Achieving Federated and Self-Manageable Cloud Infrastructures**. Theory and Practice, IGI-Global (2012). doi:10.4018/978-1-4666-1631-8.ch010.
14. OAuth. (2007). **Hueniverse Beginner's Guide to OAuth**. Available: http://hueniverse.com/2007/10/beginners-guide-to-oauth-part-ii-protocol-workflow
15. OneLogin. (2010). Available: http://www.justinpirie.com/2010/03/onelogin-saas-app-review-1-the-good-bad-and-ugly.
16. Peter, M., and Timothy, G., (2011). **The NIST Definition of Cloud Computing (Draft)**, Special Publication 800-145 (Draft). Recommendations of the National Institute of Standards and Technology. U.S. Department of commerce. January 2011.
17. Priebe, T., Dobmeier, W., and Kamprath, N. (2006). **Supporting Attribute-based Access Control with Ontologies**. In: Proceedings of the First International Conference on Availability, Reliability and Security. IEEE Computer Society, Washington, USA, 465-472 (2006).
18. Rasim, A., and Fargana, A., (2014). Illegal Access Detection in the Cloud Computing Environment, *Journal of Information Security*, 2014, 5, 65-71. Available http://www.scirp.org/journal/jis
19. Roshni, B., Upendra, B., and Dhiren, P. (2013). **Identity Management Frameworks for Cloud**. *International Journal of Computer Applications*, ,*83*(12).
20. Sciberras, A. (2006). **RFC 4519 – Lightweight Directory Access Protocol (LDAP): Schema for User Applications**. Internet Engineering Task Force (2006).
21. SPML. (2003). **Service Provisioning Markup Language**, Available: http://xml.coverpages.org/ni2003-06-05-a.html
22. Tewfiq, M., and Jean, S. (2007). **A Survey of "User-centric Identity Management Technologies**. In: International Conference on Emerging Security Information, Systems and Technologies, 12-17 .
23. Tusa, F., Celesti, A., Villari, M., and Puliafito, A. (2010). **Security and Cloud Computing: InterCloud**

ISSN 2278-3083

Identity Management Infrastructure. In: 19th IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises, 263-265 (2010).

24. Umme, H., Rahat, M., Muhammad, S., and Muaz, N. (2014). **Cloud identity management security issues & solutions: a taxonomy**, retrieved from http://www.casmodeling.com/content/2/1/5.
25. Wache, H., Voegele, T., Visser, U., Stuckenschmidt, H., Schuster, G., Neumann, H., and Hübner, S. (2001). **Ontology-based integration of information-a survey of existing approaches**. IJCAI-01 workshop: ontologies and information sharing, 108-117 (2001).
26. WIF. (2015). **Windows Identity Foundation**. Available: https://msdn.microsoft.com/en-us/library/ee517276.aspx
27. X.520. (2008). **ITU-T Recommendation X.520 (11/2008)**: The Directory - Selected attribute types (2008), available:
28. X.521. (2008). **ITU-T Recommendation X.521 (11/2008**): The Directory - Selected object classes (2008), available: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9599&lang=en
29. XRD. (2015). **OASIS: Extensible Resource Descriptor (XRD) V1.0**, retrieved from http://docs.oasisopen.org/xri/xrd/v1.0/xrd-1.0.html
30. XRDS. (2015**). OASIS: Extensible Resource Identifier (XRI) Resolution V2.0**, retrieved from http://docs.oasisopen.org/xri/2.0/specs/xri-resolution-V2.0.html.
31. XRI. (2015). **OASIS: Extensible Resource Identifier (XRI) Syntax V2.0**, retrieved from http://docs.oasisopen.org/xri/xri-syntax/2.0/specs/cs01/xri-syntax-V2.0-cs.html.
32. Zeilenga, K. (2006). **RFC 4524 – COSINE LDAP/X.500 Schema**. Internet Engineering Task Force (2006).