International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 4, April - 2014

A Survey on Identity and Access Management in Cloud Computing

Nida[1], Pinki[2], Harsh Dhiman[3], Shahnawaz Hussain[4]
[1, 2, 3,4] M.tech (CSE), School of Computing Science and Engineering, Galgotias University, Greater Noida, India

***Abstract*- Cloud computing is one of the most emerging technology in today's scenario which aims to provide on-demand scalable access to computing resources over the internet via cloud vendors to multi-tenant organizations. Cloud computing provides a way through which an organization can increase their computing capabilities and infrastructure facilities dynamically as and when required. While cost and On-demand availability are the top two benefits of cloud, but various trust and security issues are becoming the top concerns for the cloud computing users. In federated identity management environment, federated identity as a useful feature for Single Sign-on (SSO) and user management has become an important part. Some of the problems in federated identity management environment are platform trustworthiness, management of multiple digital identities, identity theft. Security assertion markup language (SAML), OAuth, OpenID is the main concepts in cloud authentication and federated environment. This paper addresses the issue of Identity and Access Management (IAM) under the cloud computing security head.**

Keywords- ***Cloud Computing, SSO, OpenID, Oauth, Identity federation, IAM, provisioning, Identity federation standards.***

I. INTRODUCTION

Cloud Computing is a technology which aims to provide on-demand scalable services over the Internet via Cloud vendors to multi-tenant organizations. Cloud Computing is defined by the National Institute of Standards and Technology (NIST) as *"a model for enabling 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"* [1]. The Cloud concept is defined by five main characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service [25]. With the ever increasing technological advancement, cloud computing has emerged through different services such as, software as-a-service (SAAS), Platform as-a service (PAAS), Infrastructure as-a service (IAAS).Firstly, Software as-a Service: is a software delivery model in which software and associated data are centrally hosted on the cloud and is typically accessed by the users using a thin client via a web browser. Secondly, under Platform as-a Service: a computing platform such as operating system is provided to the end user on the monthly rental basis and thirdly, Infrastructure as-a Service: they are availed by the end users which are provided by the cloud computing vendors on agreed basis for specific duration and price[2]. Cloud computing has several deployment models, namely, Private cloud: in which the cloud infrastructure is operated solely for a specific organization, and is managed by that organization only, Public Cloud: Here the resources are shared by all users in a common space and it is owned by cloud provider, Hybrid cloud: It combines the features of both private as well as public cloud and allow an organization to run some application on private whereas some on public clouds [3, 4]. There are basically five security issues in Cloud Computing Security Risks in Cloud Computing that should be considered and included in the typical Service Level Agreement (SLA) content. These are: privileged user access, data location, data disposal and e-investigations and protective monitoring, data segregation [8].

An identity is a set of unique characteristics of a user: an individual, a subject, or an object. An identity used for identification purposes is called an identifier [5]. An Identity Management System (IDM) supports the management of multiple digital identities, their authentication, authorization, roles, and privileges within or across system. It also decides how to disclose personally identifiable information (PII) and service specific user credentials of any user.IDM has various components such as: Directory services, Access management, Password administration including single sign-on, Identity authentication, User provisioning, Roles management and Federated identities, which enables the creation of virtual communities of customers and partners that can conduct business on different websites with a single log-in [6, 7].

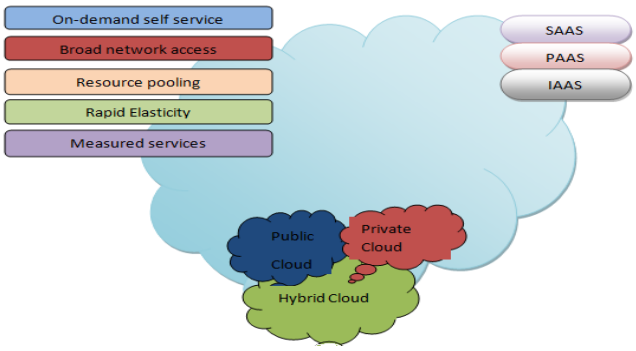

Figure 1: Cloud Computing

II. IMPORTANCE OF IDENTITY MANAGEMENT IN CLOUD

With the technological growth of cloud computing, web applications have migrated towards clouds and have raised the concerns for privacy and security of user specific sensitive data, like how can an end user or consumers verify that a service provider conform to the privacy laws and protect consumer's digital identity. Most of the service providers (e.g., Gmail and Google Maps are offered by Google) require the username/password security token to authenticate consumers but that leaves the consumer vulnerable to phishing attacks. To address this problem Identity Management (IDM) System can be used to provide the solution. IDM solution should help any user in making a suitable choice about how and what personal information user disclose, manage and control how user information can be used, cancel user subscription to any service, and keep tracking to verify that a service provider applies essential privacy policies[26]. Most of the emphasis has been laid down on how to enable a more secure authentication event through the mechanisms like Active Directory or Shibboleth, which is a key component of securing the transaction between Identity Providers (IdP) and Service Providers (SP) [27].

IDM in cloud computing environment is an essential activity as large number of consumers and services are used. Many cloud consumers are accessing and using the cloud based services on a large scale, which comes up with security concerns of user data. Therefore, monitoring, storing, managing and controlling user identities is very crucial security concerns and requires a trust based solution[29]. In an effort to understand the failures (and limited successes) of preceding identity management systems, Kim Cameron proposed seven *laws of identity* that he claims are essential for successful identity management systems[9]. They are:

1. *User Control and Consent*: An IDM system must obtain a user's permission to discover information that identifies the user.
2. *Minimal Disclosure for a Constrained Use*: An IDM system that exposes less identifying information and inforces more limits on its use is preferred.
3. *Justifiable Parties*: An IDM system must be designed so that identifying information is revealed only to parties having a essential and justifiable need.
4. *Directed Identity*: An IDM system must sustain global identifiers for use by public entities and local identifiers for use by private entities.
5. *Pluralism of Operators and Technologies:* An IDM system must sustain interoperability of multiple identity technologies executed by different identity providers.
6. *Human Integration*: An IDM system must employ unambiguous human-machine interaction mechanisms that forbid identity-based attacks (example: phishing and impersonation).
7. *Consistent Experience across Contexts*: An IDM system must provide a simple, uniform experience to users while supporting multiple operators and technologies.

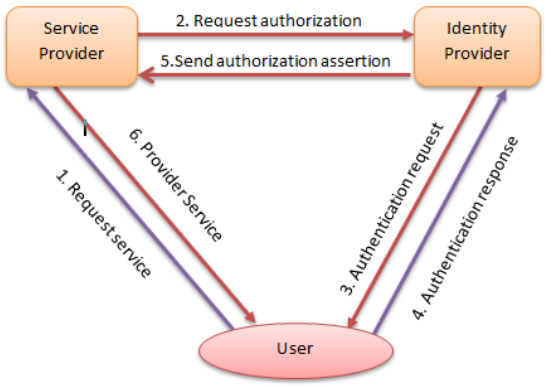

Figure2: Interaction process between SPs and IDPs during authorization phase

III. RELATED WORK

Nowadays, the area of federated identity and access management has attracted attention by various authors in the literature. A survey realized by International Data Corporation (IDC) in August 2008 consolidates the idea that security is still a barrier for the cloud users. In this context, real security incidents have happened in the Cloud Computing systems (e.g. in 2008,there were outages in Amazon Web Services, AppEngine and Gmail)[10].In the recent development it has been found that Federated identity security is gaining more attention among the researchers and it has attracted huge capital investment in industries such as Tivoli in IBM[28].Based on the related research an Identity Management Framework helps in the alignment of Identity Management initiatives with the organization's business goals and security strategy. IDM also deals with issues related to privacy, Integrity, Confidentiality of data, Provisioning/De-provisioning, user authentication and authorization. The IDM framework comprises of following components:

A. SSO

Web Single-Sign On is one of the advantages provided by the SAML standard, because a user authenticated to one web site (Identity provider), can access directly another web site (Service Provider), as is related in Fig: 3. The authentication details of the user will be recognized by the service provider, who took them from the identity provider, with the specification that between the identity provider and the service provider exist a trust relationship. The user's information between the two web sites is transferred by the SAML standard [11].Establishment of trust relationship between two web sites (called partners) and the process of sharing users personal identifiable information (PII) between them creates a *federated identity* for that user.

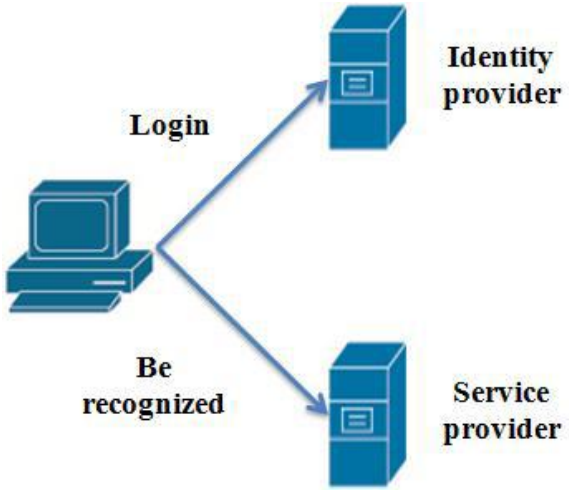

Figure 3: Single Sign-On [11]

Somorovsky et al investigated fourteen models of SAML standard and they founded many security problems that related to Extensible Mark-up Language (XML) signature wrapping. WS-Security and REST based SSO use SAML assertion for making security statement between subjects [13]. Wang performed security analysis of three commonly
available SSO, which include Microsoft Passport, OpenID 2.0 and SAML 2.0. He highlighted some Vulnerabilities and security issues for each system with their applications. He further analyzed Privacy Aware Identity Management and Authentication for the Web (SAW) as two alternative solutions for SSOs [12].According to the Yan et al, who has proposed a cryptography based federated identity with some desirable features, to adapt with cloud computing. They harmonized hierarchical identity-based cryptography with federated identity management in the cloud environment [14].

B . SAML

SAML is an XML-based framework, which was developed by OASIS Security Services Technical Committee (SSTC). The feature of SAML standard is to transfer the information about identity, authentication, attribute and authorization between organizations [16].SAML was started in 2001, uses protocol XML, HTTP, and SOAP in which user registration is not required. Its main purpose is to provide Single-sign-on for enterprise users and currently used in Google Apps.SAML has one or more strengths such as: Dominant standard, Distributed model (federation), Life cycle attributes of ID-FF, Privacy attributes of Shibboleth, Browser based identity Federation but, it doesn't address identity requirements of web services. The Consortium for defining SAML standard and security is OASIS (Organization for the Advancement of Structured Information Standards).There is three SAML versions: SAML 1.0, SAML 1.1 and the new major version of SAML is 2.0 became an official OASIS standard in March 2005. The Component of SAML is assertions, Protocols, Bindings and Profiles. [13]. A SAML protocol could be used for ensuring the identity federation of the company's users and one of the advantage of SAML protocol is its ability to interoperate with other identity federation protocols.
A SAML entity consists of two parties: *SAML asserting party* and a *SAML relying party*. The SAML asserting party or SAML authority is characterized by the SAML assertions that it does. SAML relying party utilizes the accepted assertions. Two SAML entities could collaborate by sending and receiving a request. The entity that sends the request is called *SAML requester* and the one that receive it is called *SAML responder* [16]. Examples of cloud services providers which support the SAML standard
are: Ping Identity, IBM Tivoli, CA Federation, and Juniper Networks.

C. OpenID

OpenID was started in 2005, current version OpenID 2.0 and protocol used XRDS, HTTP in which user registered is not required. Its main purpose is to provide Single-Sign On for consumers and currently used in Google, Yahoo, Facebook. OpenID is a Safe, Faster, and Easier way to Sign IN to websites. OpenID is a decentralized model for identity management, which allows service providers to delegate the authentication of users to identity providers. In this model, the identity of a user is represented by a URL, called an OpenID identifier. Hence, users don't need to create a separate account for each site; rather, they just have to use their OpenID identifier, and the authentication procedure will be conducted through the user's identity provider [15].

D. OAuth

OAuth was started in 2005, OAuth 2.0 appears last year, and it is having a fast expansion. OAuth is a user-centric open authorization standard which provides for third party a limited access to the user's web resources and it does not require an authentication procedure. The latest version of OAuth gives access to a large category of consumers (i.e. web browsers, desktop applications and smart phones).Its main purpose is to provide the API authentication between applications and protocols used JSON, HTTP. The open source OAuth 2.0 libraries and the OAuth2.0 compatible cloud sites (e.g. Facebook, Twitter, and Salesforce) prove its development [17].
In cloud computing paradigm, the parties involved by OAuth authorization protocol are: Cloud service provider, OAuth third party and the user (Figure: 4).Firstly the third party wants to obtain the request token from OAuth cloud service provider. Authorization is made by the OAuth user and then the request token is exchanged between the third party and the cloud service provider. This shows the crucial capability of OAuth: to allow the users to control the access of their resources by authorizing the access.

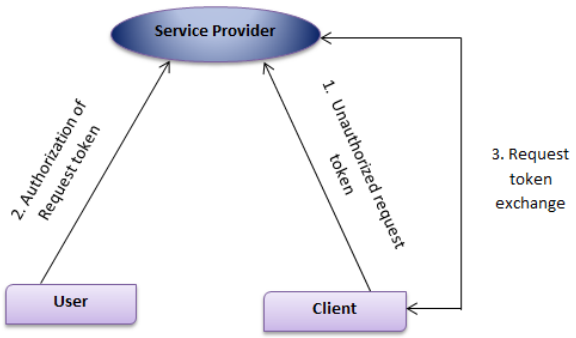

Figure 4: OAuth token exchange

E. PRIME

PRIME (Privacy and Identity Management for Europe) is a User-controlled privacy-enhancing mechanism through which an individual user can control his/her personal identifiable information (PII) as much as possible. Basically, three parties are involved in PRIME: 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 a special type of service provider is certifying authority that issues certificates that is digitally-signed statement. The PRIME involves four cryptographic tools namely secure communication, anonymous communication, pseudonyms, credentials and proofs of ownership of credentials [18].Its main purpose is data minimization and is currently used in Android Apps.

F. Federated Identity and Trust

Federated Identity Management (FIM) system is a model which deals with management of multiple digital identities and allow the access to resources that is spread over companies or other security domains. A typical example of FIM is web Single Sign-on (SSO) which allow the access of multiple related and independent software systems with a single login.FIM helps to avoid replication of user identities at multiple locations and several security domains, thereby provides an easy way to manage user identities and allowing them to access information available at several related domains in a trusted mode. In federated Identity management system, a group of governing bodies share multiple identity attributes on the basis of trust relationship and agreed-upon standards(i.e. SAML, Liberty Alliance, WS-Federation, Shibboleth) alleviating authentication from other members of federation and allowing suitable access to online resources. The foundation of FIM are trust, integrity of data and privacy of data.

Madsen et al closely examined problems in federated identity such as password attack and phishing attack. They then presented reasons and arguments that risk of identity theft increases through federated identity.FIM is conformed to accepted standards permits and simplifies the processes used by federated organizations in term of sharing user identity attributes, simplifying authentication and accessing permission using service access requirements [19]. Khattak et al have figured out the current weakness of SSO authentication and found that the misuse of user identity information could occur through SSO services in IDP and SP, which could lead to identity theft. Besides, they explored trusted computing technology and elaborated how trusted computing technology helps to effectively resolve identity theft, improper use of identity information, and trust relationship concerns in FIM system [20].FIM systems can better protect user identities when they are integrated with trust negotiation concepts such as Trust-X, Automated Trust Negotiations (ATN). Trust-X is a system which includes everything for trust negotiation, providing both an XML-based language, referred to as X-TNL, and a suite of negotiation protocols.ATN are developed in an open system and facilitates the establishment of trust through the systematic disclosure of application specific credentials of both parties involved to each other[21].

IV. IDENTITY AND ACCESS MANAGEMNT

Identity and access management (IAM) is area for managing access to organizational resources.IAM is the basic building block of any informational security program and most widely interacted security areas by users. The present scenario of IAM is involved in program-based deployment and risk-driven approach, has focused entitlement management.IAM includes all user identity management, high compliance value/cost, central view of access and increased application adoption.

In today's scenario most of the researchers are driven on the three methods realized by current IAM solutions: IAM inside the cloud, IAM up to the Cloud and IAM down from the cloud [23]. The first methodology *IAM inside the Cloud* is the simplest IAM method, focuses on creating the authentication procedure on each cloud service provider (CSP), which avoids the need for remembering the different credentials for each cloud computing application. Second, *IAM up to the Cloud* was adopted by: Juniper Networks, Inc. (2009); Goulding, Broberg and Gardiner (2010) and IBM Corporation (2010).This methodology presented new challenges which make it difficult to implement because of the obstruction of accessing the auditing and reporting features in the cloud service provider. Thirdly, *IAM down from the cloud*, appears to be more appropriate for every company size but this technique also impart challenges in terms of efficiency, which are based on the obstacles imposed by the integration process of the on-premise IAM[23].

Cloud providers need to access a secure access and technical solutions, ensure that the data stored in the cloud could be made available only to authorized users, which are registered to the cloud providers. The present IAM system has following functional requirement:

i) Identity Federation
ii) Access Control
iii) Identity provisioning/de-provisioning.

iv) Authentication

i) Identity Federation

Identity federation should be taken into consideration in order to deliver for cloud service consumers the opportunity to use the same entity's identity in others cloud services, without the need to provide same entity's details again, as they will get recognized[23].

ii) Access Control

The Access Control requirement constitutes who has the access to a particular resource. It is necessary to deliver access control policy based on concerns about the privacy and security of data, depending on the user profile information.

iii) Identity provisioning/de-provisioning

Identity provisioning is the act of enrolling user's accounts or credentials to a cloud service, in secure manner and on a explicitly stated time. At the same time, that particular user account could be de-provisioned by cancel it if it's necessary. Moreover, the enterprise should be able to extend their identity management solutions to the cloud service. Identity provisioning/de-provisioning is an appropriate advantage in many situations [22].

iv) Authentication Requirement

After users account provisioning to the cloud services, the company's users could authenticate to the Cloud service, by confirming that the access identity entities which were found in the provisioning process. Authentication requirement is essential as it eliminates the attack's risks to enter into cloud services [22].

IAM Life Cycle

The management of user identity and access control permissions can be analyzed as multiple stages. The IAM life cycle (figure: 5) illustrates the stages that users follow when they join an organization and obtain access to the tools, assets required to do their jobs. The IAM life cycle also includes stages to ensure that employees hold appropriate access as they go within the organization with access being revoked or modified when they separate or change their roles.

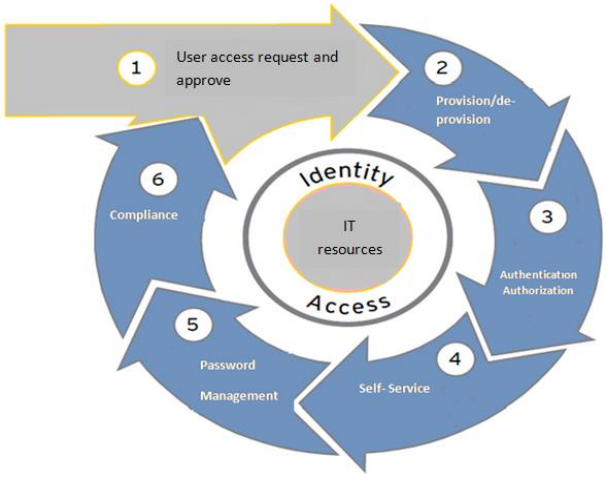

Figure 5: IAM Life Cycle

SAML 2.0 includes the identity life cycle attributes of Liberty Identity Federation Framework (Liberty ID-FF) standard and also dominant privacy functionalities of Shibboleth 1.3 standard [24].

V. CONCLUSION

Cloud Computing is an emerging technology in today's scenario, besides its overwhelming advantages the security issue under it, is still a serious concern. Security and privacy issue of user identities are major attractive areas of research. In this paper, we have discussed the concept of Cloud Computing, Identity management, its standards and framework. Further, this paper discusses Identity and access management, its requirement and existing IAM solutions. Identity and access management is essential in cloud computing and helps in the management and remote access of user's credentials.

REFERENCES

1. Mell, P., and Grance, T. 2011. The NIST definition of Cloud computing (draft), NIST. [Online]. Available: http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_Cloud-definition.pdf.
2. Suresh Kumar RG1, S.Saravanan2, Soumik Mukherjee 3," *recommendations for implementing cloud computing management platforms using open source*", IJCET, Volume 3, Issue 3, October - December (2012), pp. 83-93.
3. Sun (2009a) A Guide to Getting Started with Cloud Computing. SunWhite paper. https://www.sun.com/offers/docs/cloud_computing.
4. Cloud Computing – A Practical Approach by Velte, Tata McGraw-Hill Edition (ISBN-13:978-0-07-068351-8).
5. Angin, P., Bhargava, B., Ranchal, R., Singh, N., Linderman, M., Othmane, L. Ben and Lilien, L. 2010. An entity-centric approach for privacy and identity management in Cloud computing. In Proceedings of the 29th IEEE Symposium on. IEEE in Reliable Distributed System.
6. Wikipedia. 2010. Identity management systems. [Online].avilable:http://en.wikipedia.org/wiki/Identity_management_systems.
7. Rizwana Shaikh, M. Sasikumar, "*Identity Management in Cloud Computing*", International Journal of Computer Applications (0975 – 8887) Volume 63-No.11, February 2013.

8. Kandukuri, B.R., Paturi, R.V., Rakshit, A.: Cloud Security Issues. In: IEEE International Conference on Services Computing, Bangalore, pp. 517–520 (2009).
9. K. Cameron, "The Laws of Identity," Identity Blog, 2005;www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.
10. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee, G., Petterson, D.A., Rabkin, A., Stoica, I., Zaharia, M.: Above the Clouds: A Berkely View of Cloud Computing. Technical Report No. UCB/EECS-2009-28, Berkely Electrical Engineering and Computing Science, University of California, Berkely (2009).
11. OASIS, SAML V2.0 Executive Overview (online) OASIS (2005a), http://www.oasis-open.org/committees/download.php/13525/ Sstc-saml-exec-overview-2.0-cd-01-2col.pdf (accessed November 10, 2010).
12. Wang, "An Analysis of Web Single Sign-On," 2011.
13. J. Somorovsky, A. Mayer, A. Worth, J. Schwenk, M. Kampmann, and M. Jensen, "On breaking SAML: Be whoever you want to be," In WOOT, 2012.
14. L. Yan, C. Rong, and G. Zhao, "*Strengthen cloud computing security with federal identity management using hierarchical identity based cryptography*," in 1st International Conference on Cloud Computing, CloudCom 2009, December 1, 2009 - December 4, 2009, Beijing, China, 2009, pp. 167-177.
15. Nunez, D., Agudo, I., and Lopez, J. 2012. Integrating openid with proxy re-encryption to enhance privacy in Cloud-based identity services. In Proceedings of the IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom).
16. OASIS, Security Assertion Markup Language (SAML) V2.0 Technical Overview (online) OASIS (2008), http://www.oasis-open.org/committees/download.php/20645/sstc-saml-tech-overview-2%200-draft-10.pdf (accessed November 10, 2010).
17. Wu, W., Zhang, H., Li, Z.: Open Social based Collaborative Science Gateways. In: 11th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), pp. 554–559 (2011).
18. Roshni Bhandari, Upendra Bhoi, Dhiren Patel,*" Identity Management Frameworks for Cloud*", International Journal of Computer Applications (0975 – 8887) Volume 83 – No 12, December 2013.
19. P. Madsen, Y. Koga, and K. Takahashi, "*Federated identity management for protecting users from ID theft*," 2005, pp. 77-83.
20. Z. Khattak, S. Sulaiman, and J. Manan, "*A study on threat model for federated identities in federated identity management system*," 2010, pp. 618-623.
21. Abhilasha Bhargav-Spantzel, Anna C. Squicciarini, Elisa Bertino, "*Trust Negotiation in Identity Management*," IEEE Security & Privacy, vol. 5, no. 2, pp. 55-63, March-April 2007.
22. CSA, Top Threats to Cloud Computing V1.0 (online) Cloud Security Alliance (2010)https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf (accessed July 27, 2011).
23. Identity Federation in a Hybrid Cloud Computing Environment Solution Guide, Juniper Networks, Inc. (online) (2009), http://www.juniper.net/us/en/local/pdf/implementationguides/8010035-en.pdf (accessed February 20, 2011).
24. Identity and Access Management: beyond compliance [Online]. Available: http://www.ey.com/GL/en/Services/Advisory/Identity-and-access-management---beyond-compliance.
25. Characteristics of Cloud Computing [Online]. Available: http://www.inforisktoday.in/5-essential-characteristics-cloud-computing-a-4189.
26. Privacy and Identity Management in cloud [Online]. Available https://www.cs.purdue.edu/homes/bb/IDM-final.ppt.
27. A. Bhargav-Spantzel et al., "*Privacy Requirements in Identity Management Solutions*" ,Proc. 2007 Conf. Human Interface: Part II, Springer- Verlag, 2007, pp. 694–702.
28. IBM Corporation, IBM Tivoli Access Management for Cloud and SOA environments (online) (2010), ftp://public.dhe.ibm.com/common/ssi/ecm/en/Tis14053usen/TIS14053USEN_HR.PDF (accessed August 11, 2011).
29. Rohit Ranchal, Bharat Bhargava, Lotfi Ben Othmane, Leszek Lilien, Anya Kim, Myong Kang, Mark Linderman. Protection of Identity Information in Cloud Computing without Trusted Third Party. In proceedings of the 2010 29th IEEE International Symposium on Reliable Distributed Systems.