Identity Management in Cloud Computing –A Review

Kumar Gunjan
Dept. of Information Technology
B.I.T. Mesra, Ranchi, India

G.Sahoo
Dept. of Information Technology
B.I.T. Mesra, Ranchi, India

R.K.Tiwari
Dept. of CompSc. & Engg.
R.V.S CET, Jamshedpur, India

Abstract

The Cloud computing paradigm has gained much popularity these days because of its ability to provide highly scalable resources at cheap rates. However, the concern for security is seen as a barrier towards its adoption. In Cloud computing all the users' data is kept on the service provider's side thus arising the need for proper security measures and frameworks. Proper Identity Management may be seen as the first step towards accessing any kind of service from the clouds. It's a person's identity which authorizes him and gives rights to access some data or application in the cloud. Hence Identity theft is perceived as a severe problem and may have disastrous consequences. This paper reviews the trends and approaches taken towards a better Identity management in Cloud computing for a more secure cloud environment.

1. Introduction

Cloud computing offers us on demand network access to a shared pool of configurable computing resources (e.g., servers, storage, applications) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This paradigm has been raising great interest within both academic as well as industry communities [1]. The most popular service delivery models in cloud are software-as-a-service, platform-as-a-service and infrastructure-as-a-service. Traditionally the user generally buys a licence for the software product and then installs it on his machine. But in SaaS model, the user purchases subscription of the software product in which most of the data and code resides on the side of the service provider. For ex- Google Docs is just like Microsoft Office but is built on the lines of SaaS model. Any number of users can access it via internet and make changes to the documents. All the documents get stored on Google's server and the user just needs a browser to access it. In PaaS model, a development framework/environment is provided for the developers to write programs or build applications on it rather than doing it using their own infrastructure. For ex- Google App Engine and Microsoft Azure services. In IaaS model, users can provision servers, storage and other computing resources on demand without bothering about their maintenance, security etc which is being taken care of by the service providers. For ex- Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3).It is attractive because of its perceived economic and operational benefits. In spite of the fact that it offers great value and opportunity for organisations, several surveys of potential cloud adopters indicate security and privacy as the number one concern delaying its adoption [2].

Various approaches and models have been proposed for addressing identity management in cloud computing. The approaches include user centric IdM in place of traditional application centric model, use of trusted third parties in identifying users, identity federation solutions, protection of Identity information without Trusted Third Party etc.

The paper is organized as follows: Section 2 defines and discusses the basic terms and goals relevant to identity management and the various relevant concerns with respect to cloud environment. Section 3 discusses the existing solutions to Identity management in general. Section 4 does a review of the various proposed approaches for IdM in the Cloud. Section 5 derives conclusions out of this survey and comments on the future scope of work in this research area.

2. Identity, identity management and its importance in the cloud scenario

An identity is a set of unique characteristics of an entity: an individual, a subject, or an object. An identity used for identification purposes is called an identifier [3]. Entity identifiers are used for authentication to service providers (SPs). Identifiers provide assurance to a SP about the entity's identity, which helps the SP to decide whether to permit the entity to use a service or not [4].

Identity management (IdM) is a broad administrative area that deals with identifying individuals in a system (such as a country, a network or an organisation) and controlling the

access to the resources in that system by placing restrictions on the established identities. Identity Management can involve three perspectives [5]:

1. The pure identity paradigm: creation, management and deletion of identities without regard to access or entitlements.
2. The user access (log on) paradigm: A traditional method say for ex a user uses the smart card to log on to a service.
3. The service paradigm: A system that delivers personalized role based, online, on-demand, presence based services to users and their devices.

A set of parties use IdM and collaborate to identify an entity. These parties are [6]:

1. Identity Provider (IdP): It issues digital identities. For example debit card providers issue identities enabling payment, government issues PAN card or SSN to citizens.
2. Service Provider (SP): It provides access to services to the identities that have the right required identities. For example- a user needs to provide identity information to be able to do transactions via net banking.
3. Entity: Entities are the ones about who claims are made.
4. Identity Verifier: Service Providers send them the request for verifying claims about an identity.

An Identity management system uses one of these three identifiers [4]:

1. That are known by both the entity as well as the service provider
2. That an entity knows and can be verified by the service provider via the identity providers
3. Identifiers like biometric information

Some of the commonly agreed upon goals of identity management are [7]:

1. Security: The strength of user authentication should be increased. The IdM solutions should allow service providers to select authentication mechanisms with adequate strength according to their existing infrastructure.
2. Trust: There should be high levels of trust between consumers and service providers as well as between service providers and identity providers.
3. Cost-efficiency:Identity management solutions should be cost- efficient both to deploy and to maintain, and allow consumers and service providers to reduce their expenditure on security solutions by relying on standardized and well proven technology.
4. Simplicity: Identity management solutions should not only make it easier for the consumers and service providers to cope with the security requirements, but also make accessing service simpler and safer for the end users.

Privacy with respect to Cloud Computing

Privacy in cloud computing may be understood as the ability of a user to control what information it reveals about itself to the cloud, and the ability to control who can access that information. Many existing privacy laws impose the standards for the collection, maintenance, use, and disclosure of personal information that must be satisfied by cloud service providers. The nature of cloud computing has significant implications for the privacy of personal, business and governmental information. Cloud service providers can store information at many locations or outsource it, making it very difficult to determine, how secure it is and who has access to it [8].

A cloud service provider is a third party that keeps and manages information about or on behalf of the consumer. This gives birth to privacy or confidentiality issues. Trusting a third party requires taking the risk of assuming that the trusted third party will act as it is expected; which may not be true at all times [9].

A consumer would never like to put its data or information in the cloud if it is insecure. Any unauthorized access may lead to identity theft which may subsequently lead to dire consequences. A simple example will be-Imagine someone from the Google team or outside logs into your ‘password protected account’ and play with the personal and sensitive information inside it.

So the main problems associated with the cloud computing model can be named as [4]:

1. Loss of control: Data, applications, and resources are located with the service provider. The cloud handles identity management as well as user access control rules, security policies and enforcement. The user has to rely on the provider to ensure data security and privacy, resource availability, monitoring of services and resources.
2. Lack of Trust: Trusting a third party requires taking risks. Basically trust and risk are the opposite sides of the same coin. Some monitoring or auditing capabilities would be required to increase the level of trust.
3. Multi- tenancy: By leveraging virtualisation technologies the cloud service providers give on rent the same physical resource to multiple consumers. For example-if consumers A and B are procuring data storage services from Amazon, there is a possibility that both A’s and B’s are residing on the same Hard Disk.

Identity Management in the Cloud Computing Scenario

In the traditional application-centric [10] IDM model, each application keeps trace of entities that uses it. In cloud computing, entities may have multiple accounts associated with different SPs. Also, entities may use multiple services offered by the same SP (e.g., Gmail and Google Docs are offered by Google). A cloud user has to provide his personally identifiable information (PII), which identifies him while requesting services from the cloud. This leaves a trail of PII that can be used to uniquely identify, or locate a single entity, which—if not properly protected—may be exploited and abused. Sharing PIIs of the same entity across services along with associated attributes can lead to mapping of PIIs to the entity [10]. The main issue is how to secure PII from being used by unauthorized parties in order to prevent serious crimes against privacy, such as identity theft [8].

3. Existing solutions for Identity Management

3.1 PRIME

Privacy and Identity Management for Europe (PRIME) [11] provides privacy-preserving authentication using anonymous credentials. The user-side component uses protocols for getting third party (IdP) endorsements for claims to relying parties (RPs). Anonymous credentials are provided using an identity mixer protocol (based on the selective disclosure protocol) that allows users to selectively reveal any of their attributes in credentials obtained from IdP, without revealing any of their information. The credentials are then digitally signed using a public key infrastructure.

A major limitation of PRIME is that it requires both user agents and SPs to implement the PRIME middleware, which hinders standardization.

3.2 Windows CardSpace

Windows CardSpace [12] is a plug-in for Internet Explorer 7, in which every digital identity is a security token. A security token consists of a set of claims, such as a username, user's full name, address, SSN etc. The tokens prove that the claims belong to the user who is presenting them.

The CardSpace framework is criticized due to its reliance on the user's judgment of the trustworthiness of an (Relying Party) RP. Most users do not pay attention when asked to approve a digital certificate of an RP, either because they do not understand the importance of the approval decision or because they know that they must approve the certificate in order to get access to a particular website. RPs without any certificates at all can be used in the CardSpace framework (given user consent). Even if an RP presents a higher-assurance certificate, the user still needs to rely on an IdP providing that certificate to the RP, thus the user needs to trust the IdP. Another drawback is that, in a case where a single IdP and multiple RPs are involved in a single working session, (which we expect to be a typical scenario) the security identity metasystem within the session will rely on a single layer of authentication, that is, the authentication of the user to the IdP. If a working session is hijacked or the password is cracked the security of the entire system is compromised [4].

3.3 Open ID

OpenID [4, 7, and 13] is an open, decentralized, free framework for usercentric digital identity management. It takes advantage of already existing internet technology (URL, HTTP, SSL, Diffie-Hellman) and realizes that people are already creating identities for themselves whether it be at their blog, photo stream, profile page, etc. They can easily transform existing URLs into an account which can be used at sites which support OpenID logins.

Its major advantages of are:

1. Highly distributed
2. Flexible – users can keep identity even when identity provider disappears (using delegation with their homepage URI as identity to different identity providers)
3. Lightweight solution

OpenID has been termed "phishing heaven" due to its susceptibility to phishing attacks and social engineering. A malicious attack can be easily set up to lure users into entering their authentication information at a website that poses as an OpenID provider website [14, 15].

3.4 Higgins

Higgins [16] is an open-source framework and collaborative project which among other things develops components that can be used to build the different parts of an identity management system. There are two major categories of Higgins components (1) Lower-level components can be used to create identity services such as attribute services, token services and relying party Web-sites (i.e., service providers) and services.(2) Upper-level components can be used to create user-centric applications which allow the user to view, employ and manage his/her various identities (i-cards).

More specifically, Higgins' upper-level components can be used to build identity agents which allow users to accept icards from card issuing sites (i.e., identity providers), they can be used to create self-issued cards, manage a user's set of cards and to use these cards towards service providers (relying parties) or local applications.

3.5 Liberty Alliance

Liberty Alliance [17] specifies open standards for identity management. The specifications define sets

of protocols that collectively provide solutions for identity federation management, cross-domain authentication and session management. The specifications also define provider metadata schemas that may be used for making a priori arrangements between providers.

The Liberty architecture contains three actors: Principal (the end user), identity provider (IdP) and service provider (SP). The Principal has an identity provided by an IdP. A SP provides services to the Principal. Once the Principal is authenticated to the identity provider, the IdP can provide an authentication assertion to the Principal, who can present the assertion to the SP. The Principal is then also authenticated to the service provider if the SP trusts the assertion. An identity federation is said to exist between an identity provider and a service provider when the service provider accepts authentication assertions regarding a particular Principal from the identity provider. The specifications allow the identity of the Principal to be federated between the identity provider and the service providers without requiring the Principal to re authenticate and can support privacy controls established by the Principal.

4. Review of existing approaches to Identity Management in Cloud environment

Angin et al. [4] proposes an entity-centric approach for IDM in the cloud. The approach is based on: (1) active bundles—each including a payload of PII, privacy policies and a virtual machine that enforces the policies and uses a set of protection mechanisms to protect themselves; (2) anonymous identification to mediate interactions between the entity and cloud services using entity's privacy policies. The main characteristics of the approach are: it is independent of third party, gives minimum information to the SP and provides ability to use identity data on hosts which may not be trustworthy.

Bhargava et al. [9] proposes an approach for IDM, which is independent of TTP and has the ability to use identity data on un-trusted hosts. The approach is based on the use of predicates over encrypted data and multi-party computing for negotiating a use of a cloud service. It uses active bundle—which is a middleware agent that includes PII data, privacy policies, a virtual machine that enforces the policies, and has a set of protection mechanisms to protect itself. An active bundle interacts on behalf of a user to authenticate to cloud services using user's privacy policies. The proposed solution is prone to attacks. E.g., the active bundle may also be not executed at all at the host of the requested service. In this case its data is not disclosed but the user is denied access to the service that he requests.

Celesti et al. [18] presents a reference architecture which is able to address the Identity Management (IdM) problem in the InterCloud context and shows how it can be successfully applied to manage the authentication needed among clouds for the federation establishment. The paper proposes a distributed system based on the IdP/SP model and is composed of hundreds of IdPs interacting with clouds' authentication module. Considering such infrastructure the home cloud and the foreign cloud represent respectively the subject and the relying party, whereas the IdP acts as the third party asserting to a foreign cloud the trustiness of the home cloud identity.

Huang et al. [19] proposes an identity federation solution, "identity federation broker", to address the multi-lateral federations among in-cloud services, external services, and on-premise apps. The solution enables transitive federation based on brokered trust model. With transitive federation, service provider only needs to configure once to support potential federation with other services and on-premise apps. In the meanwhile, subscribers have full control over cross service access, which actually triggers configuration over transitive federation between services in a transparent way. Moreover, the solution is extensible to adapt to different kinds of identity federation protocols and identity management systems of services or on-premise apps. Potentially, the broker in the solution could act as an arbitrator to solve the disputes about cross service accesses.

Huang et al. [20] analyzes the danger of sharing clear text ID profiles between different clouds. To solve this problem, they design a PPID protocol in which ID and service are divided, so third party service cloud and service provider cloud can utilize user information without sacrifice user's ID privacy.

5. Conclusion

This paper presents the concepts concerning identity, identity management and reviews the trends and approaches towards better identity management in cloud computing. However, the work done in this area of cloud computing is still in its nascent stage, and the future scope of work will be towards building a framework for an even better Identity management in cloud computing.

6. References

[1] H.Takabi,James B.D. Joshi,Gail-Joon Ahn;"SecureCloud: Towards a Comprehensive Security Framework for Cloud Computin Environments";34th Annual IEE Computer Software and Applications Conference Workshops;2010

[2] Daniele Catteddu, Giles Hogben, (ENISA report) "Cloud Computing: Benefits,risks and recommendationsfor information security". (http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport)

[3] A.Josang and S. Pope;User Centric Idenity Management;In Proc AusCERT,Gold Coast, May 2005.
[4] P.Angin,B.Bhargava,R.Ranchal,N.Singh,M.Linderman,L.B.Othmane,L.Lilien;"An Entity-centric Approach for Privacy and Identity Management in Cloud Computing",29th IEEE International Symposium on Reliable Distributed Systems;2010.
[5] S.Subashini, V. Kavitha;"A survey on security issues in service delivery models f cloud computing";Journal of Network and Computer Applications;2011.
[6] K.Cameron and M.B.Jones;"Design Rationale behind the Identity Metasystem Architecture";Jan 2006. http://research.microsoft.com/en-us/um/people/mbj/papers/Identity_Metasystem_Design_Rationale.pdf
[7] T.A. Johansen,Ivar Jorstad,D.van Thanh;"Identity managment in mobile ubiquitous environments";The Third International Conference on Internet Monitoring and Protection;2008.
[8] R. Gellman;Privacy in the Clouds:Risks to Privacy and Confidentiality from Cloud;World Privacy Forum;2009.
[9] B.Bhargava,R.Ranchal,M.Linderman,L.B.Othmane,L.Lilien,A. Kim,M. Kang;"Protection of Identity Information in Cloud Computing without trusted Third Party",29th IEEE International Symposium on Reliable Distributed Systems;2010.
[10] A.Gopalakrishnan;Cloud Computing Identity Management;SETLabs Briefings,Vol 7, 2009.
[11] S. Fischer-Hubner, and H. Hebdom, "PRIME - Privacy and Identity Management for Europe," accessed in Aug. 2010.
[12]]W. Alrodhan and C. Mitchell. Improving the Security of CardSpace, EURASIP Journal on Info Security Vol. 2009.
[13] OPENID, http://openid.net/, 2010.
[14] K. Cameron, Identity Weblog. 2010.http://www.identityblog.com/?p=685
[15] C. Sample and D. Kelley. Cloud Computing Security:Routing and DNS Threats. 2009. http://www.securitycurve.com/wordpress/
[16] "Higgins", http://www.eclipse.org/higgins/index.php
[17] Wason, T. (ed.), "Liberty ID-FF Architecture Overview, Version 1.2",Liberty Alliance Project, online: http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications
[18] Antonio Celesti, Francesco Tusa, Massimo Villari and Antonio Puliafito;"Security and Cloud Computing: InterCloud Identity Management Infrastructure";Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises;2010
[19] He Yuan Huang, Bin Wang, Xiao Xi Liu, Jing Min Xu, 'Identity Federation Broker for Service Cloud', International Conference on Service Sciences, 2010.
[20] Xin Huang, Tingting Zhang, Yifan Hou, 'ID Management among Clouds', First International Conference on Future Information Networks, 2009.