Identity Management in Cloud Computing

Rizwana Shaikh
SIES Graduate School of Technology,
Nerul, Navi Mumbai,

M. Sasikumar
Center for Development of Advanced Computing,
Kharghar,Navi Mumbai

ABSTRACT
Cloud computing offers a rich set of services by pay per use basis. The features and technology offered by various providers created a great competitive market for the business. The various security issues are attracting attention, one of which is identity and privacy of the cloud user. Users are varied about the privacy of information which they have given to the provider at the time of registration. We present an analysis of various identity management systems and proposing a simple trust based scheme for a cloud computing application and service.

General Terms
Cloud Computing, Identity, Identity Management, Trust.

Keywords
Cloud Computing, Identity, Identity management System, Trust.

1. INTRODUCTION
Cloud Computing is a type of computing infrastructure that consists of a collection of inter-connected computing nodes, servers, and other hardware as well as software services and applications that are dynamically provisioned among competing users. Services are delivered over the Internet or private networks, or their combination. The cloud services are accessed over these networks based on their availability, performance, capability, and Quality of Service (QoS) requirements. The focus is to deliver reliable, secure, fault-tolerant, sustainable and scalable services, platforms and infrastructures to the end-users. These systems have goals of providing virtually unlimited computing and storage and hiding the complexity of large-scale distributed computing from users. Thus cloud computing is a new way of delivering services.

Identity management (IDM) is defined as an integrated concept of process, policies and technologies that enables authoritative source to accurately identify entities and control the use of information between them. Identities corresponds to the entities and consisting of attributes and identifiers. An identity management describes the management of individual identities, their authentication, authorization, roles, and privileges within or across system. An identity management system is the information system that can be used for Identity management. Various components of the system are; Directory services, Access management, Password administration including single sign-on, Identity authentication, User provisioning, Compliance auditing, Role 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.

The technologies used for implementing IDM are as follows;

- Active Directory is a directory service created by Microsoft for Windows domain networks.
- Security Assertion Markup Language is an XML-based open standard for exchanging authentication and authorization data between security domains, that is, between an identity provider and a service provider
- Single sign-on is a property of access control of multiple related, but independent software systems. With this property a user logs in once and gains access to all systems without being prompted to log in again at each of them.
- OpenID is an open standard that describes how users can be authenticated in a decentralized manner, eliminating the need for services to provide their own ad hoc systems and allowing users to consolidate their digital identities.

Even though various technologies are available, there are various challenges in an identity management system. They are;

- Trusting a partner to authenticate its own users is not challenging only if that partner has solid security and user-management practices.
- Implementing the technology commonly requires customization to integrate applications and develop user interfaces.
- The most difficult task is encouragement of pervasive adoption of IDM among various organizations as explained by the author in [1].

Various cloud users are accessing and using cloud services. These users are identified by their credentials like username, password, and certificates of user, Biometric or SSN etc. These credentials vary depending on the cloud provider's identity management system. Some have provisions for only username and password, some with other credentials. These identities are stored at separate, private and confidential storage in the cloud environment. The stored information of the user can be tampered or modified by malicious or unauthorized users. Storing and managing of identities is very crucial security concerns form cloud provider side, to gain confidence form the user and also to the cloud user to increase their trust towards a cloud provider. Therefore a strong identity management system for a cloud application is the attracted by various organizations. Here we are proposing a trust based system to achieve user confidence for a cloud service. Paper is organized as follows. Section 2 deals with related research in identity management, section 3 is used to

propose the trust based scheme and section 4 concludes the paper.

2. Related Research

The area of IDM has attracted attention by various authors in the literature. Some of them are discussed here as follows. An inclusive IDM (IIDM) perspective presented by the author in [2] implies a need for a systematic approach towards integrating usability and accessibility concerns in the design and development process. IIDM should define itself as an interdisciplinary and even trans-disciplinary approach that not simply aggregates established knowledge from various disciplines but can pave the way for new ideas, approaches and technical solutions. To minimize the display of personal data, the psychic identity will be used as discussed in [3]. It has a photograph of the holder, some kind of card number for administrative reasons and the information that its interrogator is entitled to see. It provides only those unique identifying numbers relevant to the questioner. The concept of virtual reality is used for privacy and to minimize the impact of data breaches. An intermediary model between the network-side identity federation model and the client-centric identity approach is proposed in [4]. This model is based on partially blind signature scheme. In this model, only the management of the identity federation links is transferred to the user's device and the actual authentication of the user is performed by Identity Providers (IdP) in the network. This model gives the users a full control on the identity federation links while preserving the trust relationships established between Service Providers and IdPs that enable SPs to accept authentication claims provided by the IdPs. Identity selector concept also implemented here with managed and self issued cards. In [5], a pseudonym-based signature scheme is proposed to construct practical delegation solutions for universal identity management. The pseudonym-based signature scheme provides anonymous proof of possession of credentials to protect user's privacy. In [6], author proposed a dynamic privacy-enhanced federated identity management solution for cooperation, on-demand resources provisioning and delegation in cloud computing scenarios, preserving the user's privacy. It extends SAMLv2, defining an enhanced privacy module, a new reputation protocol, and considering the Enhanced Client Profile, in order to provide an efficient identity management and access control, as well as dynamic, autonomic, and user-centric establishment of cloud federations. Experience Based Access Management as given in [8] promises broad applicability across many domains. Lots of research areas can be explored by understanding challenges in their implementation. Most federated identity management systems are limited by users' ability to choose only one identity provider per service session. A linking service proposed in [9] lets users securely link their various identity provider accounts, enabling the system to aggregate attributes from multiple authoritative sources automatically without requiring users to authenticate separately to each IdP.

An IDM suitable for a single system is not desirable most of the time, since services from multiple providers can be shared and accessed by their respective users. Therefore the concept of federated IDM is essential to fully understand the user requirements in a distributed cloud computing environment.

2.1 Federated IDM

Federation is an identity management model in which various tasks associated with an identity transaction, are distributed among the actors involved in the transaction. Actors must be confident that the others performed their assigned tasks with appropriate diligence. The typical example of a federated transaction is Web single sign-on (SSO). In [10] author defined assurance as the degree of confidence an relying party can ascribe to the assertions made by some Identity Provider with respect to users' identity attributes. Many assurance frameworks were discussed and analyzed along with protocols. Identity management and privacy is discussed in terms of price discrimination by the authors [11]. Some control over how user identities and attributes are established and revealed to others becomes a tool for privacy protection and balancing of information hiding and sharing economically. Privacy enhancing strategies that aim to provide anonymity and pseudonymity are discussed. Unitary and composite approaches of providing identities were discussed by the author in [12]. By discussing special purpose and general purpose identity systems author has proposed the solution that is based on the combined approach of unitary and composite identities.

In a cloud computing environment Identity management is the essential activity as large number of customers and services are used. Many cloud users are accessing and using cloud services. Therefore storing and managing of identities is very crucial security concerns and requires a trust based solution as discussed in the next section.

3. Proposed System

In a cloud computing system federated Identity management concept is essential along with the strong and trusted Identity management system itself. Identity management systems discussed in the previous section is not sufficient for the cloud environment. A trust based solution can be proposed as follows.

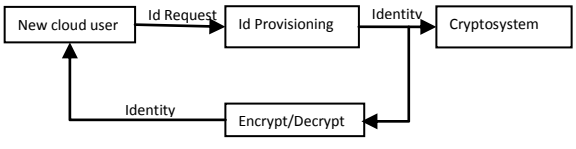

Figure 1 IDM for a Cloud Service

The various components are;

1) Identity Provisioning: At the time of new user service request, user is allowed to access and fill provisioning form which includes name, password etc. Along with that an identity is created based on combination of

numbers and character in a random fashion. The trust value associated with it can be calculated based on size, character combination with numbers and any special symbols used. Depending on the trust value user can select their identity with their own choice. The system is responsible for checking the duplicates.

2) Cryptosystem: The identities and related user credentials can be stored at some isolated location or storage. The storage should be created and maintained only by the authorized user or administrator. To increase the strength of the stored identity and identity system, it is required to maintain the strength of stored information. It should be stored and accessed by an administrator as a cryptosystem, which requires cryptographic keys and algorithms for using it.
3) Communication Channel: Created identities are passed in the encrypted form to the user while accessing the service, by the cloud provider's identity management system. Communication Security Strength depends on Strength of communication encryption key for passing identities to users, and Strength of used standard like soap message encryption strength. The system itself is responsible for encryption and decryption without involving the user.

3.1 Federated IDM

In a cloud computing environment federated Identity concept is essential as many cloud providers share their services to fulfill their respective customer needs. Therefore managing of various users identities in such environment is difficult and challenging task. Existing system already had the concept of federation, but it is for non-cloud applications. For cloud application a trust based federated identity management can be proposed as follows. The concept of federation can be implemented using static and dynamic approaches. For static one method of encryption, pseudo identity and proxy signature can be used. For dynamic approach an on demand method of provisioning is desirable. At any point of time during the cloud service usage, if the customer requires more resources that are not available with the current provider then it can be requested from others. At this moment, on time service is considered, the requested user is forwarded to other providers system for which the user identity needs to be verified by the new provider by using SAML V2 identity management. For multiple request and service usage the log records are maintained with the provider. These log records maintain the user transaction details along with the login and logout time. User access pattern of service is recorded and based on the user's previous transaction history, new access pattern is defined.

4. Conclusion

Security and privacy issue of user identities has been identified as active area of research. Various non cloud systems are identified and discussed. Identity management issue is crucial for cloud computing environment. The remote access and management of user credentials are creates privacy concerns. Many approaches are available, but we presented a simple and trust based scheme for the cloud computing application and service.

5. References

[1] Kathy Bergsma (University of Florida) on September 23, 2009.

[2] Lothar Fritsch & Kristin Skeide Fuglerud & Ivar Solheim "Towards inclusive identity management", October 2010, Springerlink.com.

[3] David G. W. Birch, "Psychic ID: A blueprint for a modern national identity scheme", Identity Journal Limited 2009.

[4] Sébastien Canard · Eric Malville · Jacques Traoré, "A client-side approach for privacy-preserving identity federation", Identity Journal Limited 2009.

[5] Yang Zhang and Jun-Liang Chen, "A Delegation Solution for Universal Identity Management in SOA", Computing, Vol 4, No 1, January-March 2011.

[6] R. Sánchez et al., "Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing", 96 IEEE Transactions on Consumer Electronics, Vol. 58, No. 1, February 2012.

[7] Rohit Ranchal et al, "Protection of Identity Information in Cloud Computing without Trusted Third Party", 29th IEEE International Symposium on Reliable Distributed Systems, 2010.

[8] Carl A. Gunter et al," Experience-Based Access Management, A Life-Cycle Framework for Identity and Access Management Systems" IEEE Computer and Reliability Societies,2011.

[9] David W.et al, "Attribute Aggregation in Federated Identity Management",IEEE Computer Society, May 2009.

[10] Paul Madsen and Hiroki Itoh, "Challenges To Supporting Federated Assurance", IEEE Computer Society, 2009.

[11] Alessandro Acquisti, "Identity M anagement, Privacy, and Price D iscrimination", IEEE Computer Society, 2008.

[12] Daniel J.Weitzner, "In Search of Manageable Identity Systems" IEEE Computer Society, 2006.