A Survey on Privacy Enhancement in Cloud Computing using Identity Management

[1]M. Janaki , [2]Dr.M.Ganaga Durga

[1]Assistant Professor, Dr.Umayal Ramanathan College for Women, Karaikudi, Tamilnadu, India

[2]Assistant Professor, Government Arts College for Women, Sivaganga, Tamilnadu, India

Abstract - Cloud computing is a better way to increase the capabilities dynamically without the expenses spent in new infrastructure or licensing new software. Though cloud computing is providing better utilization of resources by virtualization techniques and taking up much of the work load from the user, it is fraught with security risks. Traditional identity management systems are designed to be cost effective and scalable primarily for the service providers, but not necessarily for the users, which often results in poor usability. Users are often required to memorize multiple passwords for accessing various services from different service providers. In this paper, a survey of the different security risks that pose a threat to the cloud is presented. This paper compares various identity management models and paradigms and the results are summarized in the form of table.

Keywords - *Cloud computing, security issues, identity management, federated, user-centric, personal authentication device*

1. Introduction

Today Small and Medium Business (SMB) companies are realizing the fact (i.e) simply by tapping into the cloud they can gain fast access to best business applications or drastically improve their infrastructure resources, all at negligible cost. Cloud computing extends the capabilities of existing Information Technology. Within a short period, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. Cloud providers are currently enjoying a profound opportunity in the marketplace.

However, with the rapid increase in the uptake of online services, the traditional approach to identity management is already having serious negative effects on the user experience. The providers must ensure that they get the security aspects right, for it's their responsibility if things go wrong.

The rest of the paper is organized as follows: In Section 2, we introduce cloud computing paradigm, its service models and deployment models. In Section 3, we present the ten important key security elements. In Section 4, we describe the dimensions of identity management and its related concepts. In Section 5, we explain the three traditional Identity management models (i.e.) isolated model, centralized model and federated model. Then a comparative study is done based on the attributes such as Service provider, Cross domain access, Identity storage, user control and Privacy protection. Finally the results are tabulated.

In Section 6, we compare the three types of identity management paradigms with its characteristics such as distribution, trusted domain and scalability and the results are tabulated. In Section 7, we discuss the future directions of the research and we conclude in Section 8.

2. Cloud Computing

This section provides an overview of cloud computing, its service models and deployment models.

2.1. Cloud Computing Paradigm

NIST defines "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" [1]. The cloud model is composed of five essential characteristics, three service models, and four deployment models.

The five essential characteristics are (i) on-demand self-service - A client can use computing capabilities, such as server time and network storage, as needed automatically without any human interaction with each service's provider. (ii) Broad network access – Various capabilities are available over the network and accessed through the standard mechanisms (e.g., mobile phones, laptops, and PDAs). (iii) Resource pooling - The service provider's computing resources are pooled to serve multiple clients using a multi-tenant model, with

different physical and virtual resources dynamically assigned and reassigned according to the client's demand. There is a sense of location independence and ability to specify location at a higher level of abstraction (e.g., country, state, or datacenter). (iv) Rapid elasticity - To the client, the capabilities available for provisioning often appear to be unlimited and can be bought in any quantity at any time. (v) Measured Service - Cloud systems control and optimize resource use automatically by providing a metering capability. Resource usage can be managed, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

2.2. Service models and Deployment models

The three service models are (i) Cloud Software as a Service (SaaS) - This capability is provided to the client to use the provider's applications running on a cloud infrastructure. The softwares are accessible from various client devices through a web browser (e.g., web-based email). (ii) Cloud Platform as a Service (PaaS) - This capability is provided to the client to deploy onto the cloud infrastructure by acquired applications created using programming languages and tools supported by the provider. (iii) Cloud Infrastructure as a Service (IaaS) - This capability is provided to the client to provision processing, storage, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

The four deployment models are (i) Private cloud - The cloud infrastructure is operated for an organization alone. It may be monitored by the organization or a third party and may exist on premise or off premise. (ii) Community cloud - The cloud infrastructure is shared by many organizations and supports a specific community that has shared concerns.

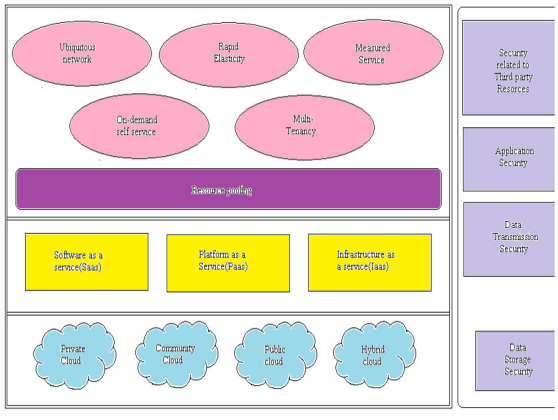

Fig 1 Cloud Computing Environment

It may be managed by the organizations or a third party and may exist on premise or off premise. (iii) Public cloud - The cloud infrastructure is made available to the general public or a large group of industries and it is owned by an organization which is selling cloud services. (iv) Hybrid cloud - The cloud infrastructure is composed of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized technology which enables data and application portability.

The Fig.1 shows the five essential characteristics, three service models and four deployment models along with the complexity in cloud security.

3. Security Issues in Cloud Computing

Though cloud computing is targeted to provide better utilization of resources using virtualization techniques and to take up much of the work load from the client, it is fraught with security risks. The complexity of security risks in a complete cloud environment is illustrated in section 2.

In SaaS, the user has to depend on the provider for proper security measures. The provider must do the work to keep multiple users from seeing each other's data stored in the cloud. So it becomes difficult to the user to ensure that right security measures are in place and to get assurance that the application will be available when needed (Choudhary, 2007). The following key security elements should be carefully considered as an integral part of the SaaS application development and deployment process:

- Authentication and authorization
- Backup
- Data security
- Data locality
- Data integrity
- Data segregation
- Data access
- Data confidentiality
- Identity management and sign-on process
- Network security

3.1 Authentication and authorization

The first key security element is Authentication and authorization. Most companies, if not all, are storing their employee information in some type of Lightweight Directory Access Protocol (LDAP) servers. In the case of Small and Medium (SMB) companies, a segment that has the highest SaaS adoption rate, Active Directory (AD) seems to be the most popular tool for managing users (Microsoft White Paper, 2010). With SaaS, the software is hosted outside of the corporate firewall. Many a times user credentials are stored in the SaaS provider's databases and not as part of the corporate IT infrastructure. This means SaaS users must remember to disable the accounts of the employees who leave the company and enable accounts as come onboard.

3.2 Backup

The second key security element is Backup. The SaaS provider needs to ensure that all sensitive enterprise data is regularly backed up to facilitate quick recovery during disasters. Also the use of strong encryption schemes is recommended to prevent accidental data leakage of sensitive information during data backup.

3.3 Data security

The third key security element is Data Security. In the SaaS model, the enterprise data is stored outside the enterprise boundary, at the SaaS vendor end. Consequently, the SaaS vendor must adopt additional security checks to ensure data security and prevent breaches due to security problems in the application or through malicious employees. This involves the use of strong encryption techniques for data security and fine-grained authorization to control data access. Malicious users can exploit weaknesses in the data security model to gain unauthorized access to data. The assessments that test and validate the security of the enterprise data stored at the SaaS are vendor Cross-site scripting[XSS], Access control weaknesses, OS and SQL injection flaws, Cross-site request forgery[CSRF], Cookie manipulation, Hidden field manipulation, Insecure storage and Insecure configuration. Any vulnerability detected during these tests can be exploited to gain access to sensitive data and lead to a financial loss.

3.4 Data locality

The fourth key security element is Data locality. The consumers use the applications provided by the SaaS and process their business data. But in this scenario, the customer does not know where the data is getting stored. In many a cases, this can be an issue. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in many enterprise architecture (Softlayer, 2009). There's the question of whose jurisdiction the data falls under, when an investigation occurs. A secure SaaS model must be capable of providing reliability to the customer on the location of the consumer data.

3.5 Data Integrity

The fifth key security element is Data integrity. It is one of the most critical elements in any system. Data integrity is achieved easily in a standalone system with a single database. Data integrity in such a system is maintained through database constraints and transactions. Transactions should follow ACID (atomicity, consistency, isolation and durability) properties to ensure data integrity. Most databases support ACID transactions and can preserve data integrity [2]. In a distributed system, there are multiple databases and multiple applications. In order to ensure data integrity in a distributed system, transactions across multiple data sources need to be handled correctly in a fail safe manner. This can be achieved using a central global transaction manager. Each application in the distributed system should be able to participate in the global transaction through a resource manager. This can be done using a 2-phase commit protocol.

3.6 Data Segregation

The sixth key security element is Data segregation. Multi-tenancy is one of the major characteristics of cloud computing. As a result of multi-tenancy multiple users can store their data. In such a situation, data of various users will reside at the same location. Intrusion of data of one user by another user becomes possible in this environment. This intrusion can be done either by hacking through the trap doors in the application or by injecting client code into the SaaS system. A hacker can write a masked code and inject in to the application. If the application executes this code without verification, then there is a high potential of intrusion into client's data. A SaaS model should ensure a clear boundary for each user's data. The boundary must been sure not only at the physical level but also at the application level. The service should be intelligent enough to segregate the data from different users [2]. A malicious user can use application vulnerabilities to bypass security checks and access sensitive data of other tenants. The assessments that test and validate the data segregation of the SaaS vendor in a multi-tenant deployment are SQL injection flaws, Data validation and In secure storage. Any vulnerability detected during these tests can be exploited to gain access to sensitive data of other tenants.

3.7 Data Access

The seventh key security element is Data access. This issue is mainly related to security policies provided to the users while accessing the data. For example, a small business organization can use a cloud provided by some other provider for carrying out its business processes. This organization will have its own security policies based on which each employee can have access to a particular set of data. The security policies may entitle some considerations wherein some of the employees are not given access to certain amount of data. These security policies must be adhered by the cloud to avoid intrusion of data by unauthorized users (Blaze et al., 1999; Kormann and Rubin, 2000; Bowers et al., 2008).

3.8 Data confidentiality

The eighth key security element is Data confidentiality. Cloud computing involves the sharing by users of their own information on remote servers owned by others and accesses through the Internet. Cloud computing services exist in many variations, including data storage sites, video sites, tax preparation sites, personal health record

websites and many more. The entire contents of a user's storage device may be stored with a single cloud provider or with many cloud providers. Whenever an individual or any other entity shares information in the cloud, privacy or confidentiality questions arise.

3.9 Identity Management and Sign-on Process

The ninth key security element is Identity management and sign-on process. Identity management (IdM) or ID management is a broad administrative area that deals with identifying individuals in a system (such as a country, a network or an organization) and controlling the access to the resources in that system by placing restrictions on the established identities. Each user will be provided certain privileges on shared data. We will consider this security issue as the main element in our paper and describe it elaborately in the successive sections.

3.10 Network Security

The last key security element is Network Security. All data flow over the network needs to be secured in order to prevent leakage of sensitive information. The strong network traffic encryption techniques such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS) are used for security. However, malicious users can use the loop holes in network security configuration to sniff network packets. The assessments that test and validate the network security of the SaaS vendor are Network penetration and packet analysis, Session management weaknesses, Insecure SSL trust configuration. Any vulnerability detected during these tests can be exploited to hijack active sessions, get access to user credentials and sensitive data.

4. Dimensions of Identity Management

This section describes the Identity management which is the most important cloud computing security issue. The evolution of cloud computing from numerous technological approaches and business models such as SaaS, cluster computing, high performance computing, etc., signifies that the cloud IDM can be considered as a superset of all the corresponding issues from these paradigms and many more. An IDM in cloud has to manage control points, dynamic composite/decommissioned machines and virtual device or service identities [3].

Today's cloud requires dynamic governance of typical Identity Management (IDM) issues like, provisioning/de-provisioning, synchronization, entitlement and lifecycle management. In cloud, provisioning means just-in-time or on-demand provisioning and de-provisioning stands for real time de-provisioning. Synchronization services help expedite the roll-out and expansion of federated identity management capabilities by enabling services in cloud to federate accounts and other data necessary to build up trust relations. Entitlement refers to the set of attributes that specify the access permissions and privileges of an authenticated security principal. Lifecycle management incorporates an integrated and comprehensive solution for managing the entire lifecycle of user identities and their associated credentials and entitlements. Identity management can involve three perspectives,

1. The pure identity paradigm: Creation, management and deletion of identities without regard to access rights or entitlements.

2. The user access paradigm: It is the user log-on process. For example: a smart card and its associated data used by a customer to logon to a service or services (a traditional view).

3. The service paradigm: A system that delivers role- based, online, on-demand, multimedia (content), presence- based services to users and their devices.

The Fig.2 given below shows the pattern of trusted Identity management.

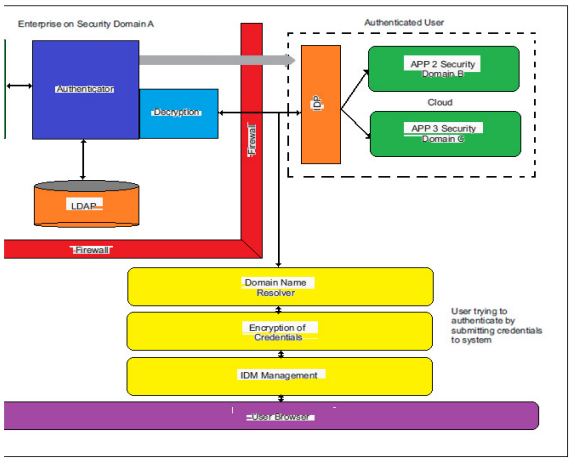

Fig 2 Trusted Identity Management

When making services and resources available through computer networks, there is often a need to know who the users are and what services they are entitled to use. Identity management has two main parts, where the first consists of issuing users with credentials and unique identifiers during the initial registration phase, and the second consists of authenticating users and controlling their access to services and resources based on their identifiers and credentials during the service operation phase [4]. A problem with many identity management systems is that they are designed to be cost effective from the perspective of the service providers (SP), which sometimes creates inconvenience and poor usability from the user's perspective.

4.1 Identity and Related Concepts

An identity is a representation of an entity in a specific application domain. For example, the registered personal data of a bank customer, and also the customer's physical characteristics as observed by the bank staff, constitute the identity of those customers within the domain of that bank. Identities are usually related to real world entities such as people or organizations. A simple assumption is that a single identity cannot be associated with more than one entity. Sometimes multiple identities may occur for the same entity in the system because of fraud. A person may of course have different identities in different domains. For example, a person may have one identity associated with being customer in a bank and another identity associated with being an employee in a company.

The set of characteristics of an identity are called identifiers when used for identification purposes. These characteristics may or may not be unique within the identity domain. They can have various properties, such as being transient or permanent, self-selected or issued by an authority, suitable for human interpretation or only by computers. The relationship between entities, identities and identifiers are shown in Fig.3 below.

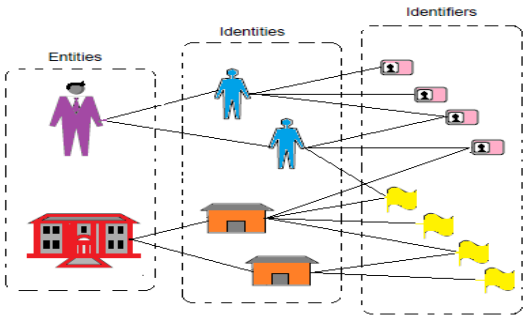

Fig 3 Correspondence between entities, identities and identifiers

This figure illustrates that an entity, such as a person or an organization, may have multiple identities, and each identity may consist of multiple characteristics that can be unique or non-unique identifiers. An identity domain is a domain where each identity must be unique. A one-to-one relationship between identities and identifiers is only allowed in a name space domain of unique identifiers. Not every identity characteristic can be used as unique identifiers: for example, a date of birth does not uniquely identify an individual person, because two or more persons can have the same date of birth.

5. User Identity Management Models

This section takes a closer look at traditional Identity management models and current practices. The three traditional models are isolated user identity model, Federated user identity model and Centralized user identity model.

5.1 Isolated User Identity Model

The most common identity management model let service providers act as both credential provider and identifier provider to their clients. Here, they control the name space for a specific service domain and allocate identifiers to users. A user gets separate unique identifiers from each service provider whom he transacts with. In addition, each user will have separate credentials, such as passwords associated with each of their identifiers. This model is called *isolated user identity management* and it is illustrated in Fig.4 below.

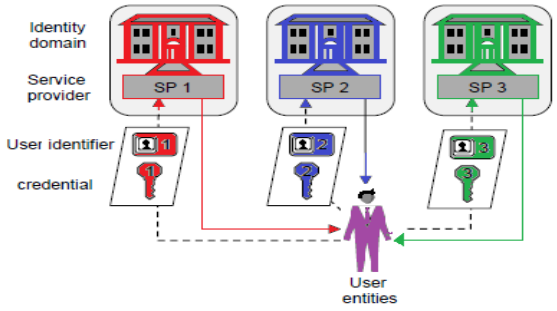

Fig 4 Isolated User Identity Model

This approach might provide simple identity management for service providers, but it is unmanageable for users. The explosive growth in the number of online services based on this model results in users being overloaded with identifiers and credentials that they have to manage. Users are often required to memorize many passwords (each one for a service). There is a chance of forgetting passwords to infrequently used services. Forgotten passwords, or simply the fear of forgetting, create a significant barrier to usage, resulting in many services not reaching their full potential. For important confidential services, where password recovery must be highly secure, forgotten passwords can also significantly increase the cost for the service providers.

5.2 Federated User Identity Model

Identity federation can be defined as the set of agreements, standards and technologies that enable a group of service providers to recognize user identifiers and entitlements from other service providers within a federated domain [4]. In a federated identity domain, agreements are established between Service Providers so that identities from different SP specific identity domains are recognized across all domains. These agreements include various policy and technology standards.

A mapping is established between the different identifiers owned by the same client in different domains that links the associated identities. This mapping results in a single virtual identity domain, as illustrated in Fig.5.

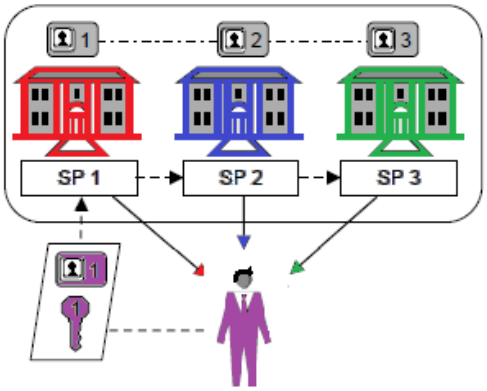

Fig 5 Federated User Identity Model

When a user is authenticated to a single service provider using one of their identifiers, they are considered to have been identified and authenticated with all the other service providers as well. This happens by passing assertions between service providers.

The federation of isolated identifier domains gives the client the illusion that there is a single identifier domain. However, he does not necessarily need to know or possess them all. A single identifier and credential is sufficient for him to access all services in the federated domain. This can therefore be used to provide a Single-Sign-On (SSO) solution.

5.3 Centralized User Identity Model

In centralized user identity models, there exists a single identifier and credentials provider that is used by all service providers. Centralized identity models can be implemented in a number of different ways such as the common identifier model, the meta-identifier model, and the single sign-on (SSO) model. The common user identity model is depicted in the Fig.6 given below.

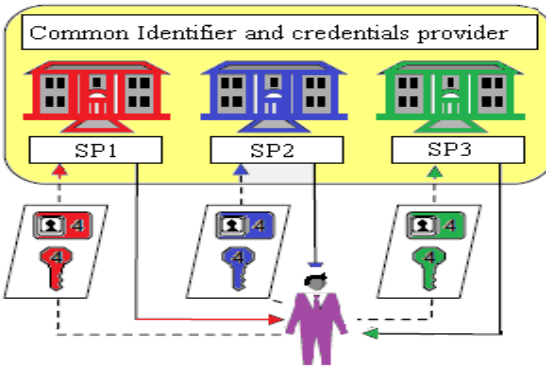

Fig 6 Common User Identity Model

A relatively simple identity management model is to let a separate entity or single authority act as an exclusive user identifier and credentials provider for all service providers. This architecture is called the *common user identity management model*. Service providers can share certain identity related data on a common, or meta, level. This can be implemented by mapping all service provider specific identifiers to a meta identifier. This architecture is commonly called the *meta user identity management model*. The model which allow a user authenticated by one service provider, to be considered authenticated by other service providers is called a Single Sign-On (SSO) solution because the user then only needs to authenticate himself (i.e. sign on) once to access all the services.

The comparative study on the three traditional identity management models (i.e.) isolated, centralized and federated models are done with the attributes such as Service provider, Cross domain access, Identity storage, user control and Privacy protection in Table 1.

Table 1 Comparison of Identity Management Models

Model	***Service Provider (SP)Type***	***Cross Domain Access***	***Identity Storage***	***User Control***	***Privacy Protection***
Isolated	Single SP	No Support	On SP	No Control	Very Weak Protection
Centralised	Multi SP	Limited Support	On IdP	Few Control	Weak Protection
Federated	Multi SP	Full Support	On both Sp and IdP	Much Control	Strong Protection

The above table shows that among the three models, Federated identity model is most advantageous but still its security arises certain risks in the cloud environment.

6. Paradigms of Identity Management

Identity management includes three kinds of paradigms which is described in this section as follows,

Network Centric Paradigm – It occurs in the early development stage of Identity management technology. In this paradigm, identity creation, management and deletion have nothing to do with the access or entitlements; the IdM system is established and operated by a single entity for a fixed user. It's not service-related or user-related. The two important challenges here are

(1) Doesn't support attributes extension and federation
(2) The semantics of the attributes haven't been take into

consideration. The example for this paradigm is Windows Domain.

Service Centric Paradigm – It composed of services from different Service Providers across multiple domains and acquires dynamic replacement of services. The two important challenges are (1) It's hard to achieve composition of services from different Service Providers and domains, these services may have quite different access control mechanisms and trust levels. (2) Delegations of user's access rights from one service to another are not easy and user's behavior is hard to track and control.

User Centric Paradigm - User is the main focus in this paradigm. Control of identity shifts from SPs to users by putting the users into the middle of transactions between Identity Provider and SPs. Users can decide which identities are needed to share with other trusted parties and under certain circumstance.

6.1 User Centric User Identity Management

An authentication solution must consider how the identifiers and credentials are to be handled by the user. If the usability is poor, then the authentication itself will be very weak because users are unable to handle their credentials adequately. In this regard, it is interesting to notice that service providers usually have automated systems to manage identities and authentication, but users normally manage credentials manually.

From a user perspective, an increasing number of identifiers and credentials rapidly become totally unmanageable. Hence we require a user centric user identity management which is illustrated in the following Fig.7.

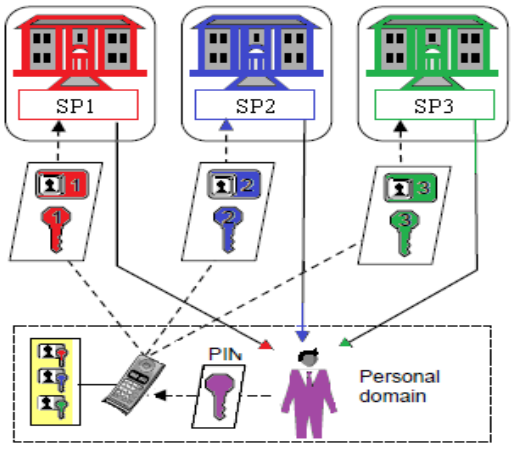

Fig 7 User Centric identity model

The PAD is a personal authentication device for identity management support; this architecture can be called user-centric identity management [4]. It can be combined with any traditional identity management model discussed above, where Fig.7 represents an example illustrating how it can be combined with the isolated identifier domains. The user must authenticate himself to the PAD, e.g. with a PIN, before the PAD can be used for authentication purposes. Many different authentication and access models can be imagined with a PAD. In case the PAD has a keyboard and display, a simple solution could let the PAD generate a dynamic password that the user then can type into the login screen of the service provider. A more advanced solution could be to connect the PAD to the client platform through a communication channel such as Bluetooth or wireless LAN. This allows the PAD to be fully integrated into the authentication process.

So far the three types of identity management paradigms and its characteristics are presented. The comparative study on them with the attributes such as distribution, trusted domain and scalability is done and the result is shown in the Table 2.

Table 2 Comparison Identity Management Paradigms

Paradigm	*Distributed*	*Trusted Domain*	*Scalability*
Network Centric	Centralized	Single	Small Scale
Service Centric	Partly Distributed	Multiple	Large Scale
User Centric	Distributed	Multiple	Large Scale

From the above table we come to know that user centric paradigm suits cloud environment well because of its distributed, multiple trusted domain and large scalability. Since the user information is stored in the user's storage the risk of identity theft is completely eradicated. This shows user centric user identity management is a better solution for cloud computing security risk regarding safe user identity storage.

7. Proposed Work

This paper describes an emerging approach, called user-centric identity management that focuses on usability and cost effectiveness from the user's point of view. Some of the identity models described above, especially the federated model, have been motivated by the need to simplify the user experience. In our view, a totally new approach is needed for the betterment of users. It seems natural to introduce automation of the identity management at the user side. Expecting users to manage an unavoidably growing number of passwords and credentials by memorization or other primitive methods is totally unrealistic.

A solution, that seems quite obvious, is simply to use the user-centric identity management model which is a new dimension in the identity management. This new approach can be framed by using an identity based cryptography which improves the user experience and of strengthening the mutual authentication between users and service providers.

Hence our proposed work primarily focuses on providing a new approach for user centric identity management to enhance privacy in cloud computing applications. This approach may be a better choice for avoiding identity theft which makes cloud environment as a better place for the users. One of the main motivations for identity management in cloud computing is to enable different services reuse user profile information.

The cloud user may no longer have to enter a lot of data for registration or wait a long time until the application has learned his preferences and can provide properly personalized services. Therefore, user centric identity management may provide functions for creating, storing and accessing digital identities (user profiles). Identity management has to clearly treat the user providing information as the owner of the profile and not the services using the information.

8. Conclusion

An integrated security model targeting different levels of security of data for a typical cloud infrastructure is under research. We intend to develop a framework to enhance privacy in cloud computing using user-centric identity management. This framework would be providing 'Security as a Service' to the applications by providing security as a single-tier or a multi-tier based on the application's requirement and addition to it, the tiers are enabled to change dynamically making the security system less predictable.

Though there are many practical concerns regarding to dynamic security, our research is much concentrated to derive a better approach which targets these concepts and provide a practical solution for the cloud computing security risks. The future direction of our research is to strengthen cloud security by using identity based cryptography in user centric identity management.

References

[1] Peter Mell, Timothy Grance, "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.

[2] Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. J Network Comput Appl (2010), doi:10.1016/j.jnca.2010.07.006.

[3] Anu Gopalakrishnan, "Cloud Computing Identity Management" SETLabs Briefings VOL 7 NO 7 2009.

[4] Audun Jøsang, Simon Pope "User Centric Identity Management", AusCERT Conference 2005. Co-operative Research Centre for Enterprise Distributed Systems Technology (DSTC) through the Australian Federal Government's CRC Programme (Department of Education, Science, and Training).

[5] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia "Above the Clouds: A Berkeley View of Cloud Computing" Technical Report No. UCB/EECS-2009-28. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html

[6] R. Buyya, et al., Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems (2009), doi:10.1016/j.future.2008.12.001.

[7] Qi Zhang , Lu Cheng, Raouf Boutaba "Cloud computing: state-of-the-art and research challenges" J Internet Serv Appl (2010) 1: 7–18. DOI 10.1007/s13174-010-0007-6 © The Brazilian Computer Society 2010, Springer.

[8] Siani Pearson "Taking Account of Privacy when Designing Cloud Computing Services", HP Laboratories, HPL-2009-54. ©Copyright 2009 Hewlett-Packard Development Company, L.P.

[9] Jian wang, Yan zaoh, Jiajin le "Providing Privacy Preserving in Cloud Computing", 978-1-4244-7562-9/10/$26.00 ©2010 IEEE.

[10] Deyan Chen, Hong Zhao "Data Security and Privacy Protection Issues in Cloud Computing" 2012 International Conference on Computer Science and Electronics Engineering. 978-0-7695-4647-6/12 $26.00 © 2012 IEEE. DOI 10.1109/ICCSEE.2012.193.

[11] Wayne Jansen, Timothy Grance "Guidelines on Security and Privacy in Public Cloud Computing" Special Publication 800-145 (Draft). Recommendations of the National Institute of Standards and Technology. U.S. Department of commerce. December 2011.

[12] Rohit Ranchal, Bharat Bhargava, Lotfi Ben Othmane, Leszek Lilien, "Protection of Identity Information in Cloud Computing without Trusted Third Party", 1060-9857/10 $26.00 © 2010 IEEE. DOI 10.1109/SRDS.2010.57.

[13] Gail-Joon Ahn, Moonam Ko and Mohamed Shehab "Privacy-enhanced User-Centric Identity Management", 978-1-4244-3435-0/09/$25.00 ©2009 IEEE.

[14] GailJoon Ahn, John Lam "Managing Privacy Preferences for FederatedIdentity Management", DIM'05, November 11, 2005, Fairfax, Virginia,USA.Copyright 2005 ACM 1595932321/05/0011 ...$5.00.

[15] Michael Koch, Wolfgang Worndl, "Community Support and Identity Management", Proceedings of the Seventh European Conference on Computer-Supported Cooperative Work, 16-20 September 2001, Bonn, Germany, pp 319-338 © 2001 Kluwer Academic Publishers Printed in the Netherlands.

[16] Eve Maler, Drummond Reed, "The Venn of Identity: Options and Issues in Federated Identity Management", Published by the IEEE Computer society, 1540-7993/08/$25.00 © 2008 IEEE.

[17] Abha Sachdev, Mohit Bhansali, "Enhancing Cloud Computing Security using AES Algorithm", Published by the International Journal of Computer Applications(0975-8887), Volume 67-N0.9, April 2013.

[18] Safiyyah srour, Gary Taylor, "Cloud Computing Based Cryptography", Published by the European Journal of Computer Science and Engineering, Vol.10 2013, ISSN(paper) 2668-3113 ISSN(online) 2668-3415.

[19] Zhiwei Wang, Guozi Sun, Danwei Chen, " A New definition of Homomorphic signature for identity management in mobile cloud computing" Published by the Journal of Computer and System Sciences (2013), http://dx.doi.org/10.1016/j.jcss.2013.06.010.

[20] Rohit Ranchal, Bharat Bhargava, Lotfi Ben Othmane, Leszek Lilien, Anya Kim, myong Kand, Mark Linderman, "Protection of Identify Information Cloud Computing without Trusted Third Party", Published by 29th IEEE International Symposium on Reliable Distributed Systems. DOI 10.1109/SRDS.2010.57.