2012 International Conference on Industrial and Intelligent Information (ICIII 2012)
IPCSIT vol.31 (2012) © (2012) IACSIT Press, Singapore

Towards Unified User Management for Achieving Cloud Adoption

Dr. Ramanathan Venkatraman [1+], Dr. Sitalakshmi Venkatraman [2]

[1] Evangelist, Institute of Systems Sciences, National University of Singapore, Singapore

[2] Senior Lecturer, School of Science, IT & Engineering, University of Ballarat, Australia

Abstract. Cloud Computing is receiving leading attention from IT industry and research arenas. However, the present slow user adoption of the cloud indicating its infancy is mainly due to lack of proper user management strategies, in particular towards intelligent deployment of interoperability and standards requirements that play an important role in effective and efficient use of the various cloud services offered. With the objective of addressing these issues, this paper proposes modeling of cloud users with user roles defined to intelligently deploy the cloud using unified cloud strategies. We believe that the proposed unified user management strategy framework provides a positive research step towards the end-goal of a seamless cloud adoption through a systemic understanding and a comprehensive analysis of cloud user management and interoperable models in order to enhance the cloud user experiences while engaging with cloud services.

Keywords: cloud services, user management, interoperability, unified cloud, cloud adoption

1. Introduction

Cloud computing has set very high expectations through its service-oriented paradigm that adopts on-the-demand provisioning of virtual resources and computing power. However, there are many challenges relating to policy, technology, security, guidance, interoperability and standards that have not matured enough for the long-term advancement of cloud computing [1][2]. We believe that the common identifying factor is from the user adoption perspective, and tailoring the cloud user model towards intelligently incorporating interoperability requirements would play an important role to address these challenges.

In general, there is a lack of public knowledge concerning data access and governance standards, and user management issues that impact the cloud adoption [2][3]. Recent research studies on cloud computing practice provide insights into the various user challenges that have placed cloud services at an early adoption stage [1][2][4]. While some big industry players [5][6] have attempted towards unified identity solutions, user management services are still chaotic, and they are not yet ready for the expected unification in the cloud. Some recent attempts for unified cloud standards by Google's UCI, Cisco's CloudVerse, and Microsoft's Hyper V based proposals are yet to cater to several multi-faceted identity management issues [7][8] that impact user adoption of systems. Hence, the aim of this paper is to identify user roles and management strategies for intelligently applying interoperability towards facilitating a unified cloud service.

To achieve our aim, in Section 2, we present a cloud user model that identifies the key players and their roles in the cloud implementation value chain, with due importance given to interoperability and governance policies that is lacking in other models. In Section 3, we propose a unified user management strategy framework that intelligently caters to a unified identity solution and interoperable data access across different applications and cloud services. This future-concept proposal serves as only a first step for an intelligent automation of the cloud. Finally, we provide conclusions along with future research work in Section 4.

+ Corresponding author. Tel.: + 65 6516 2517; fax: + 65 6778 2571
E-mail address: *rvenkat@nus.edu.sg*

2. Proposed Cloud User Model

A cloud is a dynamic provision of computing services/resource pools in a co-ordinated fashion. There are many players influencing the cloud implementation value chain. In this section, we identify these key players to manage and control the cloud according to the type of cloud and service level to which they are authorised and associated [9][10][11]. We model the cloud users under three categories, namely, Cloud Service Providers, Cloud Consumers and Cloud Architects. Fig. 1 shows the key players associated with the cloud user model in a typical cloud implementation value chain.

Currently, there are various IT organisations (***Cloud Service Providers***) offering hardware and software facilities in the form of 'pay as you go' services in the cloud. The typical cloud architecture involves multiple cloud components communicating with each other over application programming interfaces that are usually available as web services. This cloud architecture is extended to the client systems, which are typically web browsers and/or software applications that have access to the cloud applications, where individual users (***Cloud Consumers***) access the cloud from any remote computer or portable devices via the Internet. To these individual users, the cloud is considered as 'on-demand computing' without any knowledge of the location of the resources or where the applications are run. The hardware in the cloud (and the operating system that manages the hardware connections) is invisible. However, the cloud architecture allows application developers as well as regulators and auditor (***Cloud Architects***) to develop, deploy and run applications standards and policies, that can easily grow in capacity (scalability), work in real-time (performance), and offer good reliability and policy mechanisms. All the three types of users, namely Cloud Service Providers, Cloud Architects and Cloud Consumers have different purpose for interacting and interfacing with the cloud, and their roles are predominantly determined by the cloud service levels used.

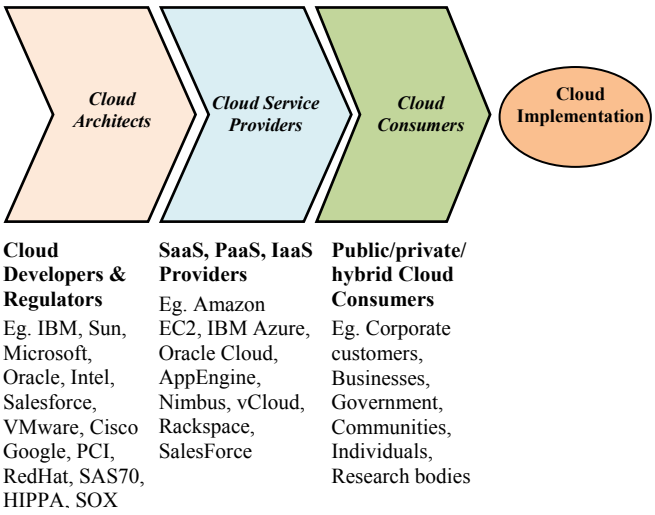

Fig. 1: Proposed cloud user model in the cloud implementation value chain

2.1. Cloud service levels and user roles

Typical cloud services include applications that cater to managing human resource, finance, customer operations, production, sales and marketing, and even affiliated business operations such as legal compliance and risks. They would also include the various services related to IT infrastructure with hardware, software and network systems as well as middleware that could offer integration, messaging, connectivity, R&D and other information tuning or performance services. Fig. 2 provides a list of typical cloud services that could be offered under three main service levels, namely, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a service (IaaS). Currently, we find that not all big players provide all these three levels of service offerings to an extent that is warranted to meet the demand of all types of consumers. Consumers, be it individual users, business users, government users or research users, would require different types of services based on their dynamically changing requirements. Typically, users would desire to have various applications in areas, such as, banking and finance, manufacturing, sales and marketing, insurance, housing, health, education, tourism, customer service, R&D, software development, etc., that could be available across different cloud services in an interoperable manner. This poses a major challenge.

Fig. 2: Typical cloud services

There are various types of users or key players identified in a typical cloud architecture. Recently, National Institute of Standards and Technology (NIST) has formulated a cloud computing reference architecture defining five major actors: Cloud Consumer, cloud provider, cloud carrier, cloud auditor, and cloud broker [1]. Each actor is an entity (a person or an organization) interacting with a cloud through a transaction or process or task. There are other consortiums that combine the terms of actors along with their roles into a common term as 'user-roles'. In this line, IBM has recently developed a set of user-roles - cloud service creator, provider, and consumer to form the basis for reflecting the close interaction among them in order to achieve the optimum service flow [4]. The main drawback in such user models is that interoperability and governance policies are not being given the deserving and explicit importance. Our premise is that though cloud provider and Cloud Consumer seem to be the common terms used in research and practice, there is a need to have a term that includes developers of cloud service, as well as regulatory parties and auditors who form another important role indirectly affecting the development of the cloud computing paradigm. Typically these regulators could be financial and system auditors, government bodies, intermediaries, law enforcement agencies or standards regulators enforcing information control and governance through policies, negotiations and standards pertaining to information format, access, privacy and other issues. We have combined these players responsible for architecting the cloud, and thereby given them a common term as 'Cloud Architects' with a view to facilitate unified cloud and to remove cloud silos.

Cloud user roles for SaaS. Typically, the SaaS level of cloud service offers various software applications to meet the needs of different users over the Web. Intelligent management and interoperability of such applications is warranted here. The Cloud Architects are responsible to develop specific applications accessible via a network to the consumers, catering to varying degrees of functional standards and policies for Web browser, Web service, and mobile Web. The Cloud Service Providers manage these cloud applications, security, and infrastructure, as well as deploy, configure, maintain, and update the operation of the software applications on a cloud infrastructure. At the SaaS service level, the Cloud Consumers have limited administrative rights. They may be able to manage certain configuration settings of applications, but do not have control on the cloud infrastructure (network, servers, operating systems, storage & applications).

Cloud user roles for PaaS: PaaS provides typical software tools such as virtualisation, database, middleware and programming compilers that are required for an application development life cycle, without the need to buy and maintain them. However, the main challenge is to provide the required flexibilility in dealing with different protocols and standards intelligently. The PaaS is a typical infrastructure platform for Cloud Architects to develop applications and policies, and connect parts of one application to parts of another application from different vendors and physical environments using common PaaS facilities and standards. While Cloud Consumers have control over the deployed applications and their hosting environment configurations, they do not manage the underlying cloud infrastructure. The Cloud Service Providers manage the computing infrastructure and run the cloud software e.g. databases, middleware components. They also support the management process of the PaaS Cloud Consumer.

Cloud user roles for IaaS: A typical IaaS level of cloud service offers various servers, storage devices and networking components and the associated operational software such as, operating systems, file systems, virtualisation technologies, etc. Cloud Architects create these services and applications, developing policies and standards to manage them. Their main role, overlooked in practice, should be in creating flexible policies to cater to different Cloud Consumer needs intelligently. For e.g., flexibility in billing based on amount/ duration of the resources consumed, flexibility in monitoring services, etc. could be achieved using data mining and machine intelligence techniques. Cloud Service Providers acquire physical computing resources, e.g. servers, networks, storage, hosting infrastructure, run service interfaces and computing resource abstractions, e.g. virtual machines & virtual network interfaces. The consumer may be allowed with limited rights to manage or control the provisioned cloud infrastructure. They have access to more fundamental forms of computing resources and control over more software components in an application stack.

3. Unified User Management Strategy Framework

An essential principle in any service design today involves understanding the skills, goals, primary tasks, and responsibilities of the user. It is noted [11] that a mismatch of user-roles and the heterogeneous requirements of technology inherently leads to systems that are more difficult to manage. User Management is an important functionality of any cloud service for its success and we propose an intelligent way of cloud deployment using unified user management strategies. Existing cloud services lack integration of user identities required in different applications, as well as in the seamless migration of existing systems and interoperability across various other cloud services. We propose that these could be intelligently addressed through the following two core components of our proposed framework as shown in Fig 3:

1. Unified User Identity Solution (UUIS) - When users have to deal with different logins for different applications and services (Fig. 2) registered with different Cloud Service Providers, there is a negative impact on the user experience that affects cloud adoption. User identity standards like OpenID [12] could provide secure authentication systems for multiple cloud services. On one hand, evolving standards with Open Authentication lead towards sharing cloud data seamlessly. On the other hand, with single sign-on and such evolving standards of Secure Assertion Markup Language (SAML), one must be aware of security breaches that are possible. Hence, strong and multi-factor authentication with SSL encryption should be enforced within cloud services. Standardised authorisation and privacy policies with intelligent ID anonymisation [13] for multiple cloud services should be developed along with automated data mining of user profiles and preferences. Such intelligent strategies would lead towards our proposed Unified User Identity Solution (UUIS).

   In our proposed UUIS based cloud deployment strategy, the role of Cloud Architects would be to move away from traditional method of associating user identity based on applications, but rather to develop new cloud applications with user identity data separated from applications so that an unified user ID could be operated across different applications and services. The Cloud Service Provider should also be able to associate this unified user ID with new applications or services offered to Cloud Consumers. The role of the Cloud Consumer is to adopt multi-factor authentication for highly secure data access across the various cloud applications and services with flexible privacy policies.

2. Unified Interoperable Resource Service (UIRS) - Another major stumbling block to cloud adoption is the lack of orchestration with existing systems and synchronisation of certain cloud services, such as e-mails, calendars, and address lists, with the existing enterprise applications [4]. Use of machine learning (ML) to process large datasets is warranted [14]. The internal silos of data and lack of standards in data control and governance need to be addressed using Unified Interoperable Resource Service (UIRS). Our proposed UIRS involves sharing and reusing user identity and profile data across multiple applications. It involves the use of service oriented architectures (SOA) in establishing components that facilitate interoperability though service interfaces, service delivery and service data repositories with intelligent capabilities for service design and lifecycle management.

   User roles for such UIRS based cloud deployment strategies are pivotal in cloud adoption. The Cloud Architects would be responsible to create a unified view of user identity using the UUIS mentioned above so that identity data could be easily shared among repositories and applications and migrated to even existing applications. Cloud Architects should design user interfaces using open standards and not tied down to building custom interfaces. Standard metadata format and APIs are needed to describe and generate eDiscovery metadata for emails, document management systems, financial account systems, etc., in order to leverage commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) software products to meet eDiscovery requirements [1][15]. This is especially important when email messaging systems, content management systems, or Enterprise Resource Planning (ERP) and financial systems are migrated to a SaaS model. In a federated multi-cloud environment with diverse cloud implementations and policies, technical policies, credentials, namespaces, and trust infrastructure must be harmonized by standards regulators to support multiple service providers. Appropriate value-added extensions to existing enterprise systems into the cloud should also be offered by cloud providers, and through UIRS their role is to orchestrate the

provisioning and configuration steps automatically. Adopting intelligent user management strategies would cater to the risk issues associated with the security, privacy and reliability of cloud services, as well as towards the availability and seamless access of information assets of Cloud Consumers. Through such an UIRS framework, Cloud Consumers could monitor the cloud services adopted by the intelligent use of transaction logs, billing according to the amount or duration of the resources consumed, such as, CPU hours of virtual computers, volume and duration of data stored, network bandwidth consumed, or the number of IP addresses used for certain intervals.

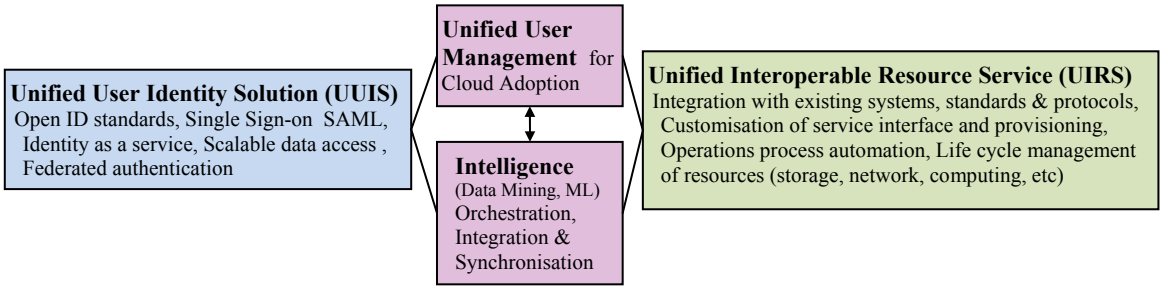

Fig. 3: Proposed unified cloud user management framework

3.1. Future unified cloud model

With the rise of mobile devices and thin clients and cheaper processors, future cloud computing will have such anywhere anytime users dominating over traditional PC based users. However, in order to support existing systems within any state-of-the-art cloud service, intelligent migration is required. Also, combined with mobile data access, there is an explosion of data that has to be intelligently managed. Hence, the next generation cloud services are aimed at intelligent solutions. For example, Cisco Intelligent Automation for Cloud [16] offers a comprehensive software solution with services for cloud users to assist in the preparation and planning, design, implementation, and optimization of cloud service offerings and delivery. However, proposed solutions do not provide due importance to the standardisation and unification of user identity and services that is warranted in cloud adoption situation that we face today and for the future. We foresee that future clouds may be deployed in the Internet as private, public or hybrid cloud, or federated clouds or virtual clusters / clouds allowing users to have broad access to various applications and services. For cloud consumers to seamlessly interact with such disparate systems and multiple vendors, our proposed service-oriented unification of these clouds through intelligent portal services would be able to integrate and manage such systems of the future. Fig. 4 depicts an overview of such a next generation service-oriented unified cloud model that is based on our proposed unified user management strategy framework described above. Artificial intelligence techniques such as, neural networks, machine intelligence, data mining would play an important part in dealing with large data from heterogeneous distributed sources and filtering meaningful information in order to facilitate a seamless and secure end-user cloud experience from virtually any location or device.

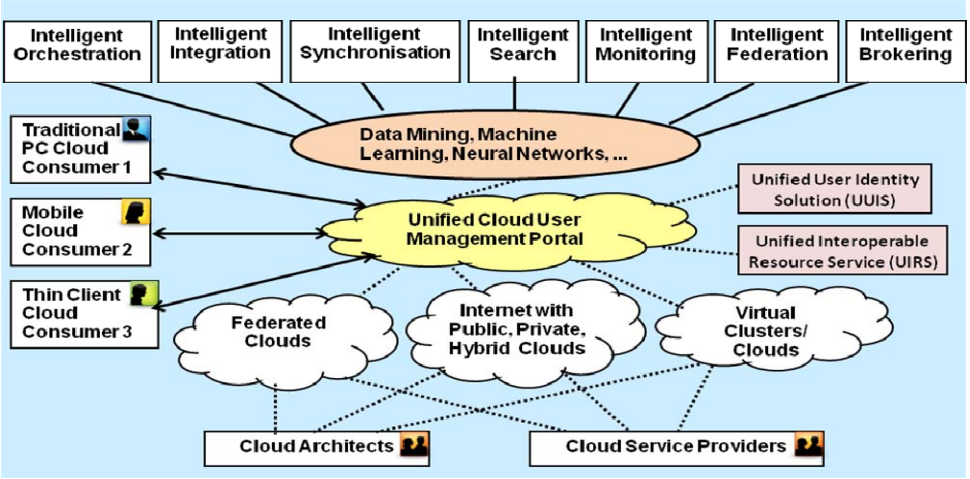

Fig. 4: Next generation service-oriented unified cloud model

4. Conclusion and Future Work

Current cloud adoption is impeded by interoperability and standards gaps, in particular from user perspectives. We have identified user roles of important players, namely, Cloud Architects, Cloud Service Providers and Cloud Consumers associated with SaaS, PaaS and IaaS, and have proposed user management strategies that can intelligently provide unified user identity solutions and services to address the prevailing cloud adoption issues. By unifying identity data across different applications and cloud services, a seamless migration of existing systems to cloud services is possible, thereby solving the complex issues of existing silos. Our unified user management strategy framework consisting of two main components, namely, Unified User Identity Solution (UUIS) and Unified Interoperable Resource Service (UIRS) would facilitate in utilising the full power of cloud computing through the achievement of interoperability, flexibility and scalability of identity data and cloud services. Future research entails in studying the coming industry trends and solutions, and the extent to which these would match and adapt with the proposed framework.

5. References

[1] NIST Report. US Government Cloud Computing Technology Roadmap, Vol. II, *NIST SP500-293*, 2011. pp. 1-85.

[2] T. Benson, Sahu, S., Akella, A. and Shaikh, A. A First Look at Problems in the Cloud, , *HotCloud '10 , 2010 USENIX Federated Conferences Week*, June 22–25, 2010, Boston, MA.

[3] V. Ramanathan and Venkatraman, S. Transforming Web and Grid Services to Cloud Services – Can it be a Success, *International Conference on Advances in Distributed and Parallel Computing (ADPC2010)*, 2010, pp. 85-90.

[4] B. Schmidt-Wesche, Bleizeffer, T., Calcaterra, J., Nair, D Rendahl, R. and Sohn, P. Cloud User Roles: Establishing Standards for Describing Core Tasks of Cloud Creators, Providers, and Consumers, *2011 IEEE International Conference on Cloud Computing*, 2011, pp. 764-765.

[5] Microsoft White Paper. 2009. Microsoft Forefront Unified Access Gateway and Direct Access, *Microsoft*, 1-14.

[6] Oracle White Paper. 2010. Oracle Identity Management 11g. *Oracle Data Sheet*. 1-4.

[7] S.D. Farnham and Churchill, E.F. Faceted Identity, Faceted Lives: Social and Technical Issues with Being Yourself Online, *CSCW 2011,* March 19–23, 2011, Hangzhou, China. 2011.

[8] J.M. DiMicco, and Millen, D.R. Identity Management: Multiple Presentations of Self in Facebook. *GROUP'*2007, Sanibel Island, Florida. 2007.

[9] W. Stuerzlinger, On- and Off-Line User Interfaces for Collaborative Cloud Services, *International Conference of Human-computer Interaction CHI 2011*, Vancouver, Canada. ACM. 2011.

[10] Väänänen-Vainio-Mattila, K., Kaasinen, E. and Roto,. V. 2011. User Experience in the Cloud: Towards a Research Agenda, *International Conference of Human-computer Interaction CHI2011*, Vancouver, Canada. ACM.

[11] J. Elson, and Howell, J. Refactoring human roles solves systems problems, *Conference on Hot Topics in Cloud Computing*, Microsoft Research. 2009.

[12] D. Thibeau, Enabling Citizen Involvement through Open Identity Technologies, *OpenID White Paper*, 2009, pp. 1-10.

[13] A. Narayanan, and Shmatikov, V. Robust De-anonymization of Large Sparse Datasets, *Proceedings of IEEE Symposium on Security and Privacy*, IEEE Computer Society. 2008.

[14] Y. Low, Gonzalez, J. Kyrola, A. Bickson, D. and Guestrin, C., GraphLab: A Distributed Framework for Machine Learning in the Cloud. *arXiv:1107.0922v1*, 2011, pp. 1-14.

[15] V. Kundra, Federal Cloud Computing Strategy. *Chief Information Officers Council Report*, USA, 2011. pp. 1-43.

[16] Cisco White Paper. Cisco Intelligent Automation for Cloud, *Cisco Data Sheet*, 2011. pp. 1-9.