Proceedings of Informing Science & IT Education Conference (InSITE) 2014

Cite as: Sutherland, S. (2014). Secure APIs and protocols to connect enterprise applications to cloud services. *Proceedings of Informing Science & IT Education Conference (InSITE) 2014* (pp. 323-336). Retrieved from http://Proceedings.InformingScience.org/InSITE2014/InSITE14p323-335Sutherland0536.pdf

Secure APIs and Protocols to Connect Enterprise Applications to Cloud Services

Susan Sutherland
University of Canberra, ACT, Australia

Susan.Sutherland@canberra.edu.au

Abstract

The is paper identifies the need for secure interoperability of application programming interfaces (APIs) and protocols for the connection of enterprise applications to cloud services, provides an overview of the researched literature that asserts the need for secure interoperability APIs and protocols, and outlines a potential solution for the use of secure APIs and protocols for the interoperation of enterprise applications and cloud services via the use of enabling technology such as service oriented architecture (SOA).

Keywords: Cloud computing, interoperability, SOA, APIs and protocols.

Introduction

With the emergence of cloud computing, the use of secure APIs and protocols to connect enterprise application systems to cloud computing has become an issue. Peer reviewed academic literature indicates that there are a number of challenges to those enterprises that migrate to cloud computing. In his research paper, Wyld (2009) argues that there are a number of challenges to those enterprises that uptake cloud computing and outlined the following challenges which potentially can impact the USA federal government in deploying cloud computing:

- scalability,
- reliability,
- security of data,
- interoperability,
- review of procurement practices,
- resolving certain political and legal issues,
- regulating cloud market,
- redefining roles of the IT Workforce,
- assessment of ROI (return on investment) of cloud computing; and
- setting up of a government cloud coordinator agency.

It is the challenge of the deployment of interoperability of secure protocols and APIs that this paper presents in relation to cloud computing and enterprise applications, as this connectivity issue has not been fully addressed due to cloud computing still being in its early stages of development. Seminal work by Bernstein, Luduigson, Sankar, Diamond, & Morrow (2009) indicates the need to open source APIs to connect applications to cloud services as currently, cloud vendors have their respective cloud services propriety con-

nections to its cloud clients thus limiting the clients from changing cloud vendors.

The rationale for the use of service oriented architecture (SOA) is that SOA is an enabling technology that forms the basis of interfaces to applications systems connecting to cloud computing. The key driver for this paper is to address a significant gap in the implementation of cloud computing, i.e., seamless connectivity of enterprise applications to cloud computing. If secure APIs and protocols are used in the deployment of cloud for enterprise applications, the following advantages could be leveraged:

- prevention of vendor locking,
- a plug and play solution for the interoperability of cloud and enterprise applications, and
- reduction of the cost of implementation.

As such, the focus of this paper is to present a potential solution for the use of secure APIs and protocols to interface applications to cloud computing. The rest of the paper explains the concept of APIs and identifies the commonly used APIs to interoperate with web 2.0 and cloud computing via SOA at the application level, and it defines the concept of cloud computing and SOA, states the gap in the use of APIs for the interoperability. The paper further provides an overview of the proposed solution as per the writer's research in progress, including the use of a proof of concept to identify security issues relating to interconnectivity as the issue of interoperability needs to be addressed to allow applications to be ported between clouds and/or use multiple cloud infrastructures before critical business applications are delivered from the cloud.

Concepts of Cloud Computing, SOA and Secure APIs & Protocols

In order to understand the need for secure APIs and protocols for the connectivity of enterprise applications to cloud services, the concepts of APIs and cloud computing and SOA need to be explained.

Applications Programming Interfaces (APIs)

The APIs and protocols referred to in this paper can be used across various tiers of cloud computing such as Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS). The concepts of PaaS, SaaS, and IaaS are discussed under the concept of cloud computing. APIs are simple commands that are understood both by the sender and receiver. There are a number of APIs in use in the deployment of Web 2.0 but the Representable State Transferable (REST) standard is the most current API standard in use. This is a web API implementation using HTTP principles.

In cloud computing, API standards are important as they allow the write once and use multiple times principle, that is, that the same commands can be used to communicate to these different applications. Based on this assumption, the proposed proof of concept will test the connectivity between enterprise applications and the vendor clouds using existing and emerging APIs.

Current implementation of connecting applications to the cloud is centred on web technologies and or high level programming knowledge. Table 1 lists some of the standards that current web services utilise and have the potential to be used for the interoperation of the cloud.

Table 1: List of Protocols and APIs for Web Services

Protocol or Interface	Standards Body if any	Purpose
XML	W3C	Represent data in SOA
Simple Object Access Protocol	OASIS	Invoke services remotely across networks and platforms
Web Services Description Language (WSDL)	W3C	Describes services remotely across networks and platforms
Universal Description Discovery and Integration (UDDI)	OASIS	Automatically publishes and discovers services
Electronic Business XLM (ebXML)	OASIS and United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT)	Automatically publishes and discovers services

The cloud APIs between vendors are not standardised as yet. While the Cloud Computing Interoperability Forum (CCIF) is working towards developing standards, the vendors are not stopping deployment. The issue is that the customers have to delay cloud implementation without locking in with a particular vendor as currently there is no inter vendor standard based interoperability as each cloud provider has its own legacy standards that have evolved with their respective product development cycle.

Lack of standard based APIs and protocols for interoperability between cloud vendors has a great impact on the enterprises where an enterprise has chosen a number of cloud suppliers to deploy its various cloud deployments. For example, an enterprise may deploy Google docs for its collaboration services including emails and another, such as MS Azure (http://www.microsoft.com/azure/servicebus.mspx), for its applications. As there is no standard based interoperability between and among cloud vendors, a given enterprise is unable to provide an integrated service to its downstream customers. It is the APIs and protocols that drive standard based interoperability between applications systems and cloud via enabling technologies such as SOA. While most of the researched literature (Lewis, 2013) suggests the need for secure APIs and protocols for interoperability between the cloud vendors and the enterprise applications, the issue of interconnectivity is also a primary concern for the downstream customers of such enterprises. Hence the author's research in progress has a focus on the secure interoperability of the convergence of cloud computing, enabling technology such as SOA, and enterprise applications. The author's research will test the interoperability between the above three distinct domains using secure APIs, protocols, and other open source code.

Cloud Computing

Cloud computing is this generation internet based, highly scalable distributed cloud applications in which resources are offered as services. There are various definitions articulated by experts of cloud computing. For the purpose of this study, a definition of cloud computing has been adopted from National Institute of Standards and Technology (NIST) and documented by Mell and Grance (2011) as per below:

Cloud computing is 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. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

The five base characteristics of cloud computing are:

- on demand,
- broad network access,
- resource pooling,
- rapid elasticity; and
- measured service

NIST identifies three of the key cloud computing services as SaaS, PaaS, and IaaS. These services are illustrated in the diagram in Figure 1 along with their respective activities:

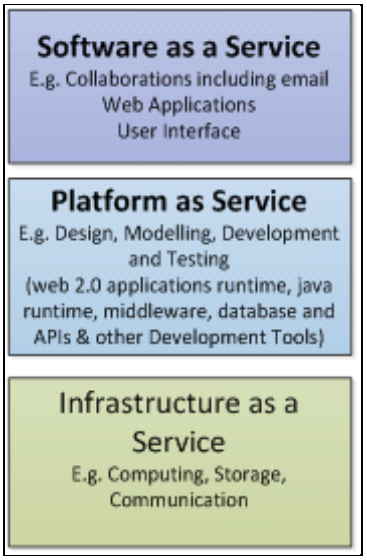

Figure 1: A Model of Cloud Computing

SaaS is where a client hosts its applications on vendor cloud and accesses the services from cloud on demand. Examples of SaaS include SalesForce.com, Google Mail, and Google Docs. *PaaS* is a development platform supporting the full applications development cycle. This allows clients to develop and host applications on the vendor cloud. The key difference between PaaS and Saas is that SaaS hosts applications for the client use whereas PaaS provides a platform work as well as allowing clients to host the developed applications. IaaS provides its cloud consumers with the full infrastructure, namely, processing, storage, networks, and other required computing resources.

The four deployment models of cloud computing as identified by NIST are:

- private Cloud,
- community Cloud,
- public Cloud; and
- Hybrid Cloud.

Service Oriented Architecture

SOA is a method of design, deployment, and the management of both applications and the software on the infrastructure where all software is organized into business services that are accessible and executable and where service interfaces are based on public standards for interoperability (Blake & Wei, 2010). SOA is also a business-driven IT architectural approach that supports integrating a business as linked, repeatable tasks or services.

The key technical concepts of SOA are:

- services,
- interoperability, and
- loose coupling.

For the purpose of this research, the author defines SOA as a set of predefined services that are held in a repository and that can be accessed dynamically when required via the use of web services technology. These services can also be discovered even if and when calls for such services are not clearly defined. These services are built on the specific procedures, policies, and framework. The services are based on protocols and can be discovered and published and are independent of platform in a non-coupling manner. Blatzan, Lynch, & Blakely (2010) summarise the protocols that are commonly used in a SOA environment as follows:

- universal Description, Discovery, and Integration, **UDDI**,
- the Web Services Description Language, **WSDL**,
- **SOAP** is the Service Oriented Architecture Protocol,
- the Lightweight Directory Access Protocol or **LDAP** , and
- extract, transform, and load, **ETL**.

The diagram below (Figure 2) illustrates how these services can be dynamically called from the repository of services:

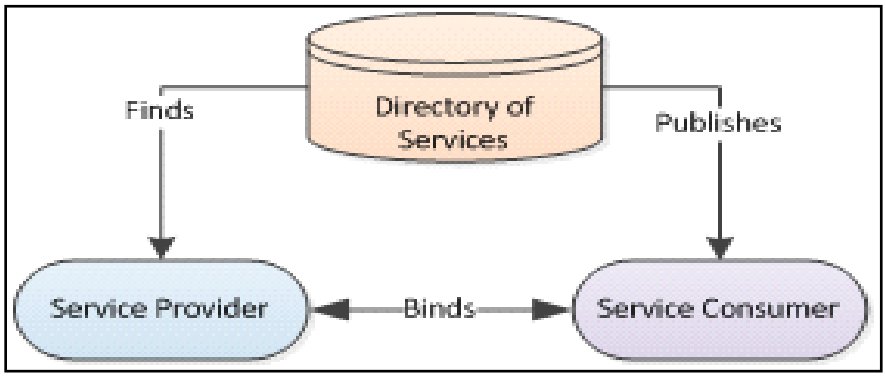

Figure 2: Services in a Cloud Implementation

Secure APIs and Protocols - Work in Progress

The Cloud Security alliance (CSA) (2010) identified top threats to cloud computing which included the following:

- abuse of cloud computing,
- insecure APIs,

- malicious Insiders,
- shared technology vulnerabilities,
- data loss and leakage, and
- account service and traffic hijacking.

The CSA works in partnership with the International Standards Organisation (ISO) to develop cloud security standards. Furthermore, enterprises that use cloud computing services are interested in security issues relating to interoperability standards, one key reason being that customers would like to move from cloud to cloud. The CCIF was formed to define how enterprises applications would interoperate with different clouds.

Seminal work by Loutas, Kamateri, and Bossi (2011) discusses the different security management standards such as Information Technology Information Library (ITIL) and International Standards Organisation (ISO). There are two other key works in progress on APIs and interoperability:

- DMTF's Open Cloud Standards Incubator (OCSI) focus on building interoperability standards between different cloud vendor offerings, and
- The open cloud computing interface working group (OCCI-WG) develops practical specifications related to IaaS.

A recent sample survey by the author (Sutherland, 2013), based on her research in progress on the standard based interoperability for cloud computing, SOA and enterprise architecture (EA), indicated that the participants have listed security of interoperability as one of the issues to migrating to cloud computing. There are a number of areas that secure interoperability is of interest to vendors, customers, researchers, and the standards bodies. Some of these areas are:

- secure interoperability between different cloud vendors such as between Microsoft Azure and Google Docs,
- secure based interoperability within a given cloud, and
- secure interoperability between enterprise applications and Cloud.

Overview of Reviewed Literature

The reviewed literature in the area of interoperability of secure APIs and protocols found two key findings, namely, the challenge of interoperability itself and the interoperability between cloud and SOA. The emergence of SOA forms the basis of highly flexible and reusable services by allowing users and developers to display discrete pieces of functionality. As this paper focusses on the emerging need for secure APIs and protocols for the interoperability of enterprise applications to cloud computing, the author's research project will utilise the existing application architectures such as SOA and lightweight APIs that are used as building blocks and open source code to set up a proof of concept for the interoperability of cloud computing, service oriented architecture and enterprise applications.

Challenge of Standard Based Interoperability

Research by Dillion, Wu, and Chang (2010) highlights the implementation issues and challenges of cloud computing. It identifies issues relating to the lack of standards that will pose implementation problems for the enterprises. In fact, the research also points out that the issue of secure interoperability protocols has not taken the centre stage as yet, as large and complex enterprises have not been drawn to the total migration of applications to cloud services.

The Cloud Computing Interoperability Forum (CCIF 2009) is working towards developing standards for cloud computing. While standards have alleviated this issue in other emerging technolo-

gies such as SOA, the issue of interoperability of standards are to be further addressed when deploying cloud computing. Kim (2012) raises the issues of vendor locking when enterprises use vendor specific solutions of cloud computing

Interoperability between Cloud Computing and Service Oriented Architecture

With the emergence of cloud computing, researchers are finding a place for SOA in the transition of existing applications to cloud computing. This no doubt will be leveraged by the protocols that emerged as part of the web 2.0 technologies, especially those that had been based on SOAP (simple object access protocol). SOAP is an XML (Extensible Mark-up Language) based on open source message transport protocol. The enabling technologies such as virtualization at the operating systems and infrastructure level could be also leveraged in the delivery of services using SOA. At a conceptual level, services will need to be identified and created in SOA. The aim of using SOA is to create a service once and use it multiple times for a variety of processing. The created service in SOA dynamically makes a call to the cloud computing services such that the processing occurs. Examples of calls for the cloud services can be found below:

- access software – SaaS,
- use disk space – IaaS, and
- access to OS for administration - PaaS

While cloud computing is a utility service, the reviewed literature confirms that there are three stacks in cloud computing, namely, Saas, IaaS and PaaS. In some instances these have been expanded as stated by Buyya, Yeoa, Venugopala, Broberga, & Brand (2009). Blake and Wei (2010) confirm that the there is an overlap of services between service oriented architecture and cloud computing. As such, the challenges for one could be leveraged as an opportunity for the other. Blake and Wei's (2010) work is also relevant to the author's research study as their research argues the application of uniform standards to achieve standard based interoperability protocols between cloud and SOA. According to these authors, the key challenge for the enterprises that wish to maintain their service directories but have decided to migrate to cloud using a propriety vendor solution is that they cannot easily change their deployed services from one cloud computing provider to another. For this reason, large and complex enterprises are not moving to cloud without the trailed and tested secure APIs and interoperability protocols that support open standards. As such, there is a need to investigate the secure APIs and protocols for the interoperation between cloud computing and enterprise applications with open standards. Furthermore, when linking enterprise applications to cloud computing, the enabling technology such as service oriented architecture (SOA) is deemed necessary to providing an end-to-end solution for creating a convergence of SOA, enterprise applications, and cloud computing.

Tang and Dong (2010) document a view of cloud services within the framework of SOA. This research focuses on a SOA centric architecture to use cloud services. This research is a significant work but this work is predominantly theoretical with no clear implementation strategy or guidelines for developing a proof-of-concept solution. For this reason, the planned research will investigate the secure APIs and interoperability protocols for the convergence cloud computing, SOA, and enterprise applications within a given cloud environment, with the development of a logical solution model and subsequent proof of concept prototype implementation.

Though Blake and Wei (2010), and Tang and Dong's (2010) work provide insight into the standard based interoperability protocols and APIs between SOA and cloud services and between different vendor clouds, they fail to extend their research in the space of secure interpretability protocols and APIs for the convergence of enterprise applications with SOA and cloud services.

Therefore, there is a gap in the space of secure interoperability protocols and APIs for the convergence of all three, namely, enterprise applications, SOA, and cloud services.

The Problem Identified

The problem identified is that there is a lack of secure APIs and protocols for a seamless connectivity between cloud and enterprise applications. More specifically, from the above, reviewed literature confirms that there is potentially interoperability between SOA and cloud computing but none of the literature reviewed suggests that dynamic interoperability exists between enterprise applications at an enterprise architecture level and SOA (Blake & Wei, 2010) to facilitate the convergence of the three entities. The problem identified is captured in a framework as developed by the author and illustrated below in Figure 3:

Methodology

In particular, the author's research project will attempt to bundle a set of APIs to form an application middleware connection, namely, Cloud Interoperability Broker (CIB), to cloud computing, thus designing a set of uniform APIs and protocols irrespective of the vendor implementations, enabling the customers of cloud to be vendor independent. In order to prove this connectivity, the author will test the capability of the APIs and protocols to develop, deploy, execute, manage, and monitor integration flows linking multiple end points. The proof of concept will utilise use cases to test such functionality across at least two vendors as identified by using a CIB including, a middleware connector such as Mulesoft (http://www.mulesoft.com) which has the ability to:

- support a variety of connectivity protocols and data/message delivery styles;
- route, and
- manage API.

Gartner's magic Quadrant (Mulesoft, 2013) on the Enterprise Integration Platform as a Service has rated Mulesoft highly as an integration tool to connect to cloud.

A solution is expected to be achieved via a proof of concept which will aim to test secure interoperability of services between SOA and Cloud and the convergence of the three entities via the use of secure APIs and protocols. The proof of concept will include the following activities:

- architect a solution based on secure APIs and protocols and emerging cloud integration software tools,
- source uses cases that will lend themselves to a cloud implementation,
- create a database of services from the use cases to be used for testing,
- set up (build) a cloud service prototype using SOA technology with an open source connectivity to vendor clouds,
- develop a testing procedure to test the transactions,
- collect the data by identifying the most common and effective paths to find and transact such services as part of the testing,
- analyse the results of the tests,
- benchmark the results against another vendor solution of cloud implementation,
- document and prepare report,
- publish the research findings, and
- arrange to pilot this proof of concept to gain further live data to complete the research project.

It is also expected that the results of the testing will highlight the typical security breaches that could occur in a given solutions. Some of these are:

- authentication and authorisation,
- availability,
- data security,
- web application security,
- data access,
- data locality , and
- data breaches.

The Proposed Solution

It is proposed to design and implement a cross platform API that is both vendor and language independent, thus provisioning the interconnection of enterprise applications to cloud services from multiple cloud vendors.

The results of the proof of concept will give a better understanding of how best to link the services between and among Cloud computing, SOA, and enterprise applications, thus setting up the convergence paths that best meet the requirements of an enterprise. The focus for the proof of concept prototype development will be on designing a set of protocols, use cases, and software tools for recommending a novel middleware connector named as **Cloud Interoperability Broker (CIB)** to be part of the cloud ecosystem. The market researchers, watchers, and analysts are unhesitatingly articulating that currently there is a huge market scope for such cloud brokerage and middleware services for assisting different types of enterprises with disparate enterprise architecture models and SOA architectures to migrate to cloud deployments. For such scenarios, the proposed CIB connector can provide a proper mapping to standards-compliant APIs and protocols for convergence of interoperability of these disparate entities and will assist enterprises towards smooth EA-SOA-CC empowered migration.

A set of use cases for evaluating the proposed CIB connector will be sourced and tested. For this, in addition to the Microsoft Azure (http://www.microsoft.com/azure/servicebus.mspx) platform, some of the open source platform tools, especially MuleSoft ESB (http://www.mulesoft.com) development suite will be investigated.

Mulesoft is a lightweight Java-based ESB (Enterprise Services Bus) and integration platform that allows developers to connect applications quickly and easily, enabling them to exchange data. Mule ESB enables easy integration of existing applications regardless of the different technologies used by the applications, including JMS, web services, Java Database Connectivity (JDBC), hypertext transfer protocol (HTTP), and more. Mule ESB includes a set of capabilities called Mule Cloud Connect, enabling the integration of enterprise data and applications seamlessly with SaaS and cloud-based web applications.

These capabilities include a set of out-of-the-box cloud connectors for popular cloud, SaaS, and Web 2.0 providers (e.g., Amazon Web Services, Salesforce.com, and Facebook), as well as providing an easy way for users to create their own cloud connectors. In addition, native REST support allows users to publish and consume REST services easily and seamlessly using Mule. Finally, AJAX/JavaScript integration enables developers to access enterprise data directly from a browser-based application without requiring heavyweight server-side infrastructure.

Conclusion and Expected Results

The following results are expected:

A Logical Model

This author's research study will provide an opportunity to develop a logical solution model for the convergence of cloud computing and enterprise applications. Such a solution model will provide a basis for a migration path to cloud computing for the enterprises that already have established enterprise architecture and the need to extend their service delivery with the deployment of cloud computing services. A conceptual model of proposed solution model is illustrated below in Figure 3:

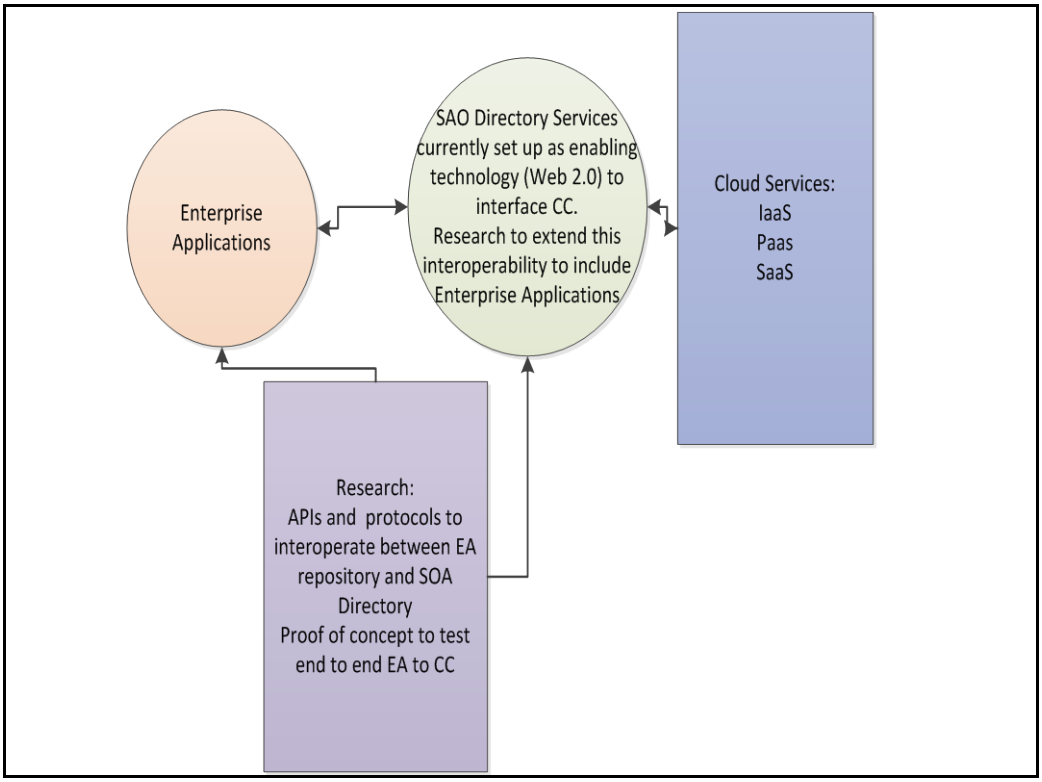

Figure 3: A Conceptual Solution for the Convergence of EA, SOA and CC

Review Enterprise ICT Architectures to Include SOA in the Delivery of Cloud Computing

This research will contribute to the redesign of EA in enterprises. With the emergence of cloud services, enterprises will be forced to examine their existing architecture framework and models to allow for seamless transactions when utilising cloud services. In doing so, enterprises will need to link their EA framework and models to the cloud services via SOA as literature reviewed clearly indicates that a transparent path for large and complex enterprises attempting to deploy cloud services is the use of SOA as an enabling technology. An overview of the interoperation scheme between SOA and cloud computing is illustrated below in Figure 4.

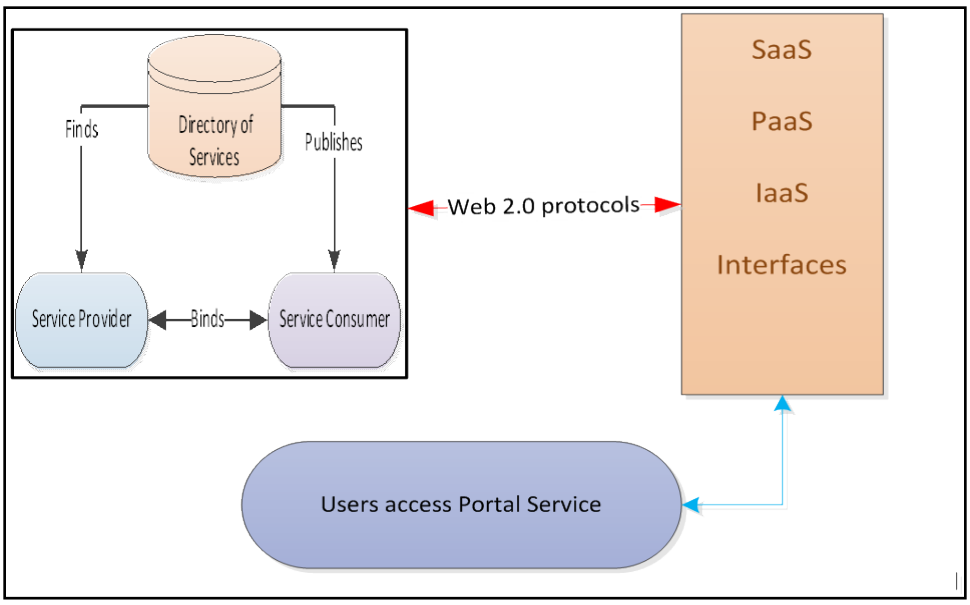

Figure 4: SOA and CC Interoperability

An internal paper by Deloitte (2010) on cloud computing states the relevance of EA in cloud computing. According to Deloitte, enterprise architecture will still have to govern how all system components work together to support business. Without a coordinated plan, it will be difficult to deliver a service over the whole network.

Test Interoperability Protocols such as XML, Web 2.0 Protocols, & Open Source Connectors.

This research will also test the standard based interoperability protocols of the convergence of protocols to complete the convergence of EA, SOA, and Cloud computing services. In migrating to cloud services, one of the key issues that enterprises will be presented with is the interoperability of CC with SOA. There are standards and technologies that will be enable this operation but there is a lack of research in the space of interoperation of enterprise architecture and the architecture technology such as SOA as outlined in the reviewed literature. As such this proof of concept will test the interoperation of EA and SOA by setting up an EA repository of services based on the enterprise architecture framework. This repository will then publish services to the SOA directory services which in turn will call the services from a cloud service. Where the existing standard based interoperability protocols fail to provide this convergence, these protocols will need to be enhanced if possible to give the proposed convergence of EA, SOA, and Cloud computing.

Other Benefits to Enterprises

This research project will, via its proof of concept, demonstrate the benefits gained by enterprises when deploying cloud services. Specifically, the enterprises when deploying cloud services will benefit from:

- a better alignment of business requirements and advocated enterprise architecture by an enterprise;
- a more agile and at the same time stringent life cycle of the cloud services transacted; and
- a potential for a tailored service level agreement between the service provided and the customers thus managing the risk of migrating to cloud computing.

Finally, as an emerging ICT trend, cloud computing will become an architectural challenge if not managed by enterprises. The Australian Government Information Management Office (AGIMO) strategic direction paper (AGIMO, 2012) provides a high level direction for cloud based implementations emphasising the benefits of using cloud. Such benefits include scalability, flexibility, availability and productivity.

References

AGIMO (Australian Government Information Management Office). (2012). *Cloud computing. Strategic direction paper 2012*.

Bernstein, D., Luduigson, E., Sankar, K., Diamond, S., & Morrow, M. (2009). *Blueprint for intercloud – protocols and formats for CC Interoperability*. Fourth International Conference on Internet and Web Applications and Services.

Blake, B., & Wei, Y. (2010). *Service oriented computing and cloud computing*. Published by IEEE Computer Society.

Blatzan, P., Lynch, K., & Blakely, P. (2010). *Business driven information systems*. McGraw Hill Australia Pty Ltd.

Buyya, R., Yeoa, C. S., Venugopala, S. J., Broberga, J., & Brand, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems, 25*(6), 599-616.

Cloud Security Alliance. (2010). *Top threats to cloud computing V1.0.* Retrieved from http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Deloite (2010). Does cloud computing make enterprise architecture irrelevant? Retrieved from http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_consulting_cloudComputingDebate_092110.pdf

Dillion, T, Wu, C., & Chang, E. (2010). *Cloud computing: Issues and challenges*, 24th IEEE International Conference on Advanced Information Networking and Applications, 2010.

Kim, W. (2012). Cloud computing today and tomorrow. *Journal of Object Technology. 8*(1), 65-72.

Lewis, G. A. (2013, January). Role of standards in cloud-computing interoperability. In *System Sciences (HICSS), 2013 46th Hawaii International Conference* (pp. 1652-1661). IEEE.

Loutas, N., Kamateri, E., & Bossi, F. (2011) *Cloud computing interoperability: The state of play*. Third IEEE International Conference on Cloud Computing Technology and Science.

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing (draft).* NIST special publication 800: 145.

Mulesoft. (2013): *MuleSoft named a "leader" in the Gartner magic quadrant for enterprise integration platform as a service (iPaaS)*. Retrieved from http://www.mulesoft.com/gartner-leaders-ipaas

Sutherland, S. (2013). *Migration to cloud computing: a survey*. ACS Newsletter, August 2013.

Tang, L., & Dong, J. L. (2010). *Enterprise cloud service architecture*. Cloud Computing (CLOUD), IEEE 3rd International Conference on, IEEE.

Wyld, D. C. (2009). *Moving to the cloud: An introduction to cloud computing in government*. IBM Centre for the Business of Government.

Biography

Susan Sutherland has some 20 years of experience in small, medium, large and complex enterprises both in private and public sectors at an operational and strategic level. She pioneered the implementation of Internet in the Australian Federal Government and is interested in the deployment of bleeding edge technologies and their migration and integration into mainstream computing. Currently she is undertaking her PhD study and does sessional lecturing. In the recent past, she has worked as a consultant in the space of internet services.