# Investigation into Interoperability in Cloud Computing: An Architectural Model

Susan Sutherland*, Girija Chetty
University of Canberra, PO Box 148 Jamison Centre ACT 2614 Australia.

* Corresponding author. Email: susan.sutherland@canberra.edu.au
Manuscript submitted February, 2015; accepted May 31, 2015.
doi: 10.17706/jcp.11.2.159-168

**Abstract:** This paper presents an architectural model that enables the convergence of the interoperability of Enterprise Architecture (EA), Service Oriented Architecture (SOA) and Cloud Services. As per the reviewed literature by the authors, there is a lack of research in this space of cloud computing. Hence the authors' research developed an innovative solution to provide a 'plug and play' architectural model to seamlessly connect the enterprise systems to cloud within the governance standards of enterprise architecture. The rest of the paper discusses the identified research problem and articulates the developed model while validating the model with a few use cases, and concluding that the research community could further validate the model with their respective application use cases.

**Key words:** Interoperability, cloud computing, service oriented architecture, enterprise architecture, architectural model.

## 1. Introduction

This paper presents an innovative model for a problem identified earlier by Sutherland [1] that there is a gap in academic literature on the convergence of Cloud Services, Service Oriented Architecture (SOA) and Enterprise Architecture (EA). This research highlighted key emerging themes in the researched literature on the interoperability cloud computing. Such themes included market oriented architecture, interoperability and disruptive technology and identified the above gap while highlighting the significance of managing risks, return on investments and Service level agreements to transition to the cloud paradigm.

The need for standard based interoperability protocols for the convergence between EA and SOA is a requirement that has been also confirmed by scholarly research by Tang, Dong and Zhao [2]. Though there is an existence of convergence of interoperability in practice between cloud computing and SOA as researched from the published scholarly material by Wei and Blake, there is no such convergence of interoperability among EA, SOA and cloud services [3]. Several research works, including the seminal work by Raj and Periasamy identified the need to set up standard based interoperability protocols between and among the EA, SOA and the Cloud [4]. The underlying theme for this convergence to occur is to use interoperability standards and protocols as per the suggested model. Further work by Sutherland suggest that, interoperability focuses on the setting up of an agreed framework/technology that enables easy migration of integration of applications and data from between different cloud systems/vendors and also facilitates for secure data exchange and integration between and among platforms within an enterprise [5].

The significance of the study was further established via a sample survey carried out [6]. The sample survey was administered on the readers of the Australian Computer Society (ACS) members within the ACT

and who are also in the strategic management positions to either influence their respective Information Communications and Technology (ICT) strategies and/or have the decision making powers to deploy cloud computing. This survey provided an overview of the significance of interoperability in the process of migrating to cloud services along with the preferred services that the enterprises needed to migrate and their preferred vendors. The results confirmed that the enterprises will need to evaluate the cloud computing services on offer against their respective requirements to ensure all enterprise architectural aspects such as interoperability, data migration and security are addressed during evaluation. This survey also confirmed that interoperability is perceived as an issue when migrating to cloud computing as most enterprises prefer not to be challenged by vendor locking issues.

## 2. Problem Discussed

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 of interoperability has become a significant factor in migrating to cloud services. Each Cloud provider has its own set of APIs to connect enterprises to cloud. Individual cloud vendor APIs have evolved over time with the respective vendor legacies and they are inherent in the vendor solutions of cloud services. Hence the significance of this research is that it identifies the current industry standards and services that will allow seamless interoperability between and among EA, SOA and Cloud Services

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 lack of 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 [7] 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.

Seminal work by Loutas, Kamateri, and Bossi [8] 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 are 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.

There are a number of areas that secure interoperability is of interest to vendors, customers, researchers, and the standards bodies. Some of these areas include secure interoperability between different cloud vendors such as between Microsoft Azure and Google Docs, secure based interoperability within a given cloud services, and secure interoperability between enterprise applications and cloud services.

However, this researched architectural model concentrates on the interoperability between enterprise applications to cloud and the interoperability of the convergence of EA, enterprise applications and the cloud services.

### 2.1. Cloud Computing Reference Architecture Models

There are number of cloud providers that deliver cloud services in the market place but when it comes to

architectural framework, vendors differ in their architectural models/framework Examples of the different models and architecture include DMTF Cloud Service Reference Architecture, IBM Cloud Computing Reference Architecture, NIST Cloud Computing Reference Architecture, Cloud Security Alliance, CISCO Cloud Reference Alliance, and IEFT Cloud Reference Framework.

For the purpose of this research paper, NIST Cloud Computing Architecture framework as illustrated below will be used as a referenced point [9]:

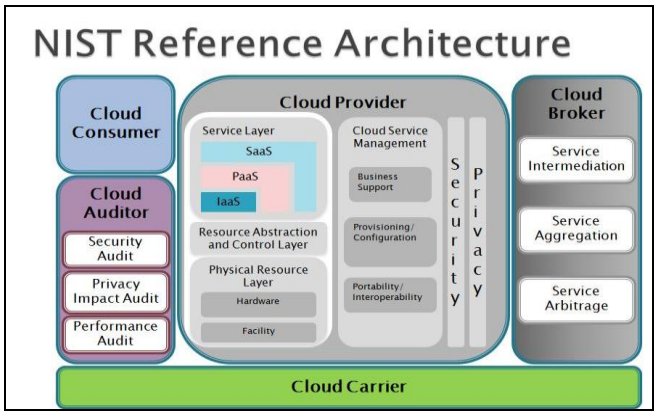


Fig. 1. Source: NIST cloud computing/architecture.

The value in using reference architecture is that it provides a consistency in such aspects in terminology, deliverable and governance across an enterprise. This also enables sensible reuse of capabilities. Based on this reference, this research has developed a base architectural model for the convergence of EA, SOA and Cloud Services.

## 2.2. Architectural Problem Being Addressed

The Fig. 2 identifies gaps in the convergence of EA, SOA and Cloud Services illustrates the problems being addressed, namely, interoperability of EA and SOA; and secondly the integrated interoperability of EA, SOA and Cloud Services.

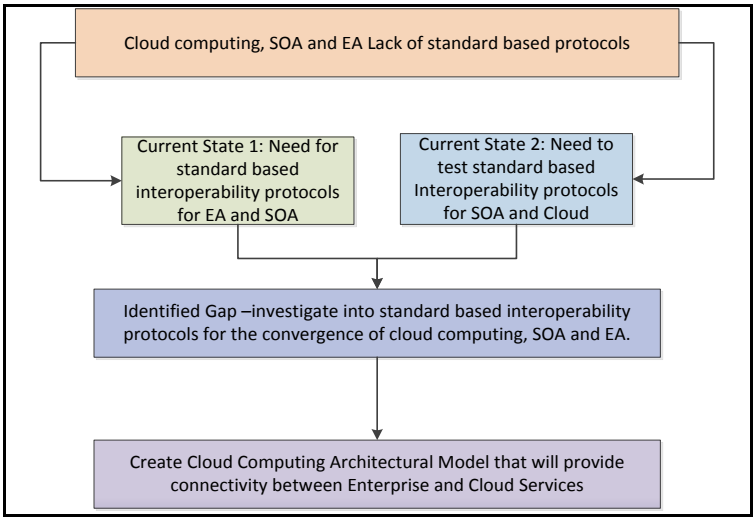


Fig. 2. Identified gaps in the convergence of EA, SOA and cloud.

## 3. The Interoperability of Convergence Architectural Model/S:

The research has developed an architectural model that has four horizontal layers and one vertical layer to conform to bring about an architectural model to address the two identified problems. This architecture will

as illustrated in the figure below (Fig. 3) provide a plug and play model such that enterprises could use multiple vendors to deliver them with multiple cloud services at the same time ensuring to have a return on investment of the existing enterprise standards. Furthermore, this model will form a strong alignment with enterprise architecture and its framework.

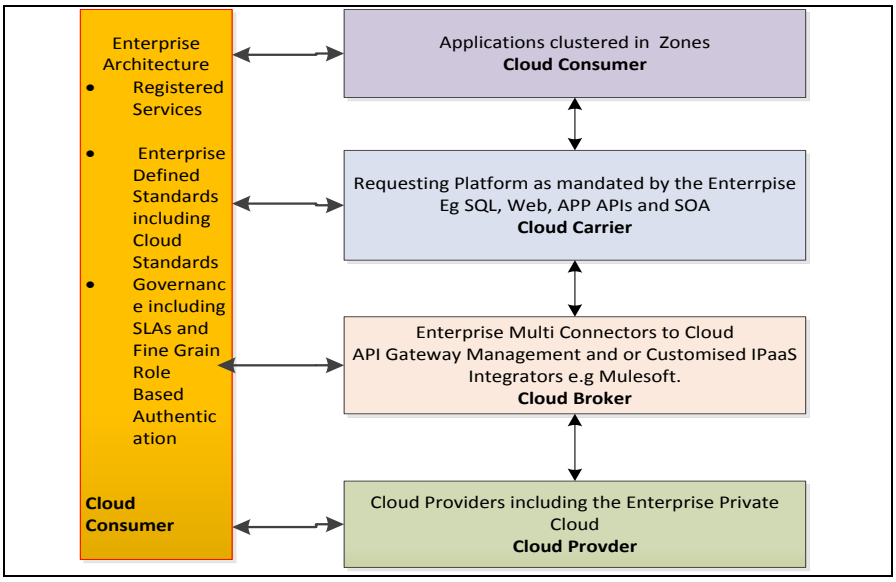


Fig. 3. Architectural model to allow multi connectors and multi-vendor.

## 3.1. Components of the Architecture Model

This model utilises one vertical layer, namely EA which includes Registered Services and Standards Definitions and four horizontal layers namely, Application Zones, Requesting Platform e.g. SQL, SOA APIs and web services; and Cloud Providers.

### 3.1.1. Enterprise architecture and services register

In this model, the Enterprise architecture supports the registration services which are basically an identified list of services that the enterprise uses to support it operations for the delivery of cloud services. These services need to be also registered with the cloud vendors as unless they are included in the Service Level Agreements with the Vendors and or unless they are also registered in the Enterprise Register of Services, services could not be released by a Cloud Vendor. Further conditions apply as where a service is required and is not in the SLA, it needs to be included in the SLA before it is released to the user; and where a service is not in the Register of Services and not in the SLA, it will need to be created and registered by the Enterprise Architect and then forwarded to the contracts department to register the services in the enterprise registry service and within the SLAs with the respective vendors.

### 3.1.2. Enterprise architecture and enterprise defined standards including clouds standards and enterprise defined services

The purpose of this component is to ensure that all standards defined by the EA are to be the standards used in the deployment of Cloud Services within the Enterprise irrespective of the vendors. This will ensure that the vendor standards are not imposing on the Enterprise architecture. The enterprise stipulates the standards that both the enterprise and cloud vendors use for delivery of cloud services within a given enterprise.

The second purpose of this component is the use of defined services only. Enterprise Architecture will define the services and list the services in the service directory for unless the services are registered in the services directory, they will not be allowed to be used. For this, enterprises will need to create a register of

services which is linked with the service level agreement (SLA) for the agreed services with the vendor. A dynamic updates needs to occur between the enterprise and vendor services whenever the SLA gets updated with a new service

### 3.2. Applications Zones

Enterprises that use self-managed Internet Gateway Services to manage the network traffic throughput also use the classifications for zoning applications that use same standards and protocols such as Web Applications, SQL Applications and SOA applications. A similar zoning is proposed for this research architecture model. This will provide a platform that will allow requests from a zone to go through the API Gateway Management Service or IPaas Integrator or the hub that utilises both the integrated services of API Gateway and IPaas.

### 3.3. Requesting Platforms

The Requesting Platforms are based on Standards such as SQL, SOA and WEB. This research study focuses on the use of SOA as a component for the convergence of EA, SOA and Cloud Computing. SOA is an architecture that allows for the structuring of an application that goes through identification of a number of functional units which can be reused many times for the delivery of an application service. Web Services provide developers methods of integrating. With the emergence of cloud computing, researchers are finding a place for SOA in the transition of existing applications to cloud services. 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). 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.

The 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 [10] summarise the protocols that are commonly used in a SOA environment which include 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**.

In using SOA, the Enterprise Architecture also stipulates the governance component of the SLA including the fine grain authorisation – that is - a user upon authentication is automatically granted access to the services and the level of services. Variation of the access and access levels need to be authorised by the Chief Architect.

### 3.4. Cloud Multi Connectors

In this research architectural model, in order for the convergence of the three to occur, the SOA needs to be the focal point of connection to the vendor cloud. *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 [3]).

The industry literature reviewed suggests that connection of enterprise systems to the cloud services can be managed via an API Management Gateway such as CA's Layers or IPaaS integrators such as Mule soft. However, the issue with both these solutions are that the focus of these two solutions is external and does not address the interoperability within an enterprise and this has been identified as problem to be resolved by this research. Since the commencement of this research, the industry offerings on the connectivity to

cloud have matured and there are two clear winners in terms of connecting to cloud. The two models being:

- A model using API Management Gateway;
- A model using IPaaS Integrator such as Mule soft or Informatics.

The authors further propose an integrated model of the above two where some of the applications could use both of these models while others only one.

### 3.5. API Gateway Management

To achieve Cloud computing interoperability, the use of standardised API is of high importance. API management software can be built in-house or purchased as a service through a third-party provider like Mashery Inc., Apigee Corp. or C.A.'s Layers. API management software tools automate and control connections between an API and the applications that use it; ensure consistency between multiple API implementations; monitor traffic from individual applications; and protect the API security procedures and policies.

More specifically, the functionality can be leveraged from an API Management Gateway to convert enterprise application services into developer friendly Restful APIs. Application services associated with common SOA style generally employ SOAP protocol whereas Web devises rely on REST. The most effective API Management Gateway solutions will include functionality for presenting enterprises as Restful. This entails using SAO to convert protocols such as SOAP to Restful APIs. This is another significance of using of SOA.

Cloud APIs present a range of new and unique security challenges that go beyond what enterprises have been used to dealing when using Web technologies. However, traditional online security solutions do not cover all the potential threats created by cloud API publishing. As such, specific API protocols need to be implemented and supported by an API Gateway as per the requirements of the enterprise and hence the need for the researched architecture model to include the architectural layer of requesting platforms which includes the APIs to be used by an enterprise.

An API Management Gateway illustration below as in Fig. 4 is how this research envisages enterprises will connect to cloud:

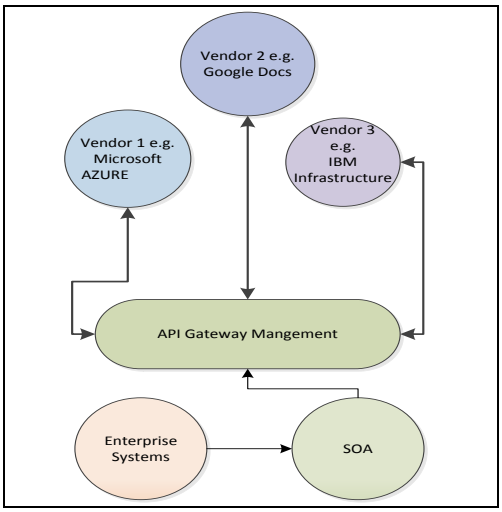


Fig. 4. Logical view of API management gateway architecture.

### 3.6. Model with Customised IPaaS Integrator Software

With this model, the enterprise invests in an IPaaS integrator that will manage the search, release and confirmation of services required by the enterprise. Some of the functionality of an IPaaS includes bridging

between a variety of connectivity protocols and data/message delivery, data/message mapping and transformation, data quality, routing, and adaptors for cloud based and on premises applications, data sources and technology,

Some industry literature suggests that the ebus architecture is the preferred method of connecting enterprise systems to cloud when using IPaaS integrators. However, there is no scholarly work that supports this. While IPaas integrators will provide seamless connection to multiple cloud vendors, it does lack the independence the enterprises could have if they created their individual gateway though there is the argument that the implementation of an IPaas integrator can be customised to maintain the enterprise standards and protocols. Hence the research model proposes mandatory use of requesting platform standards as stipulated by the Enterprise architecture; and the use of the customised IPaas integrator software such as Mule soft. Fig. 5 below illustrates a logical view of the use of IPaas integrator.

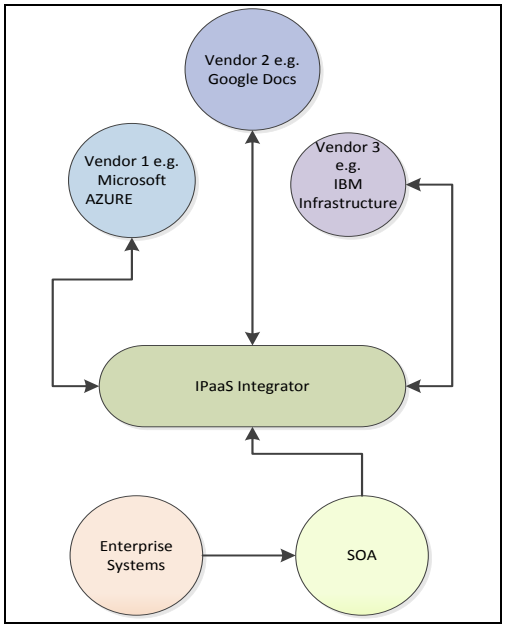


Fig. 5. Logical view of IPaaS integrator architecture.

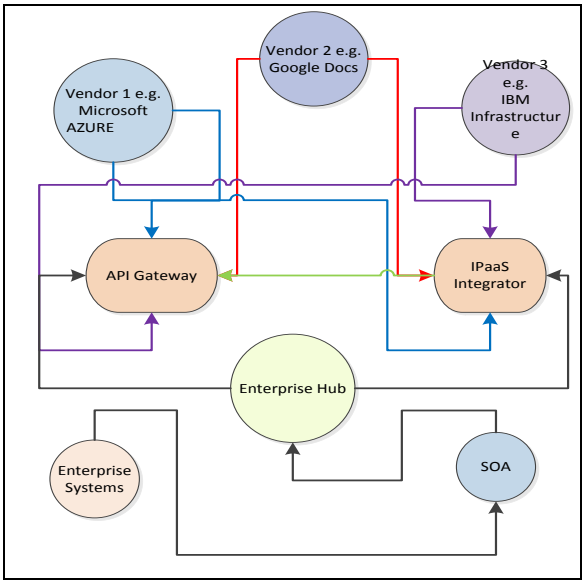


Fig. 6. An Enhanced Integrated Architectural Model of API Gateway and an IPaaS Integrator.

### 3.7. An Enhanced Integrated Model Where the API Management Gateway and an IPaas Model Based on Products such as Mules Soft

For this model to work, the zoning of applications is important as each zone can be allocated as to path it will follow, namely whether to go via the API Gateway and or via the IPaaS Integrator software. Hence the significance of the enterprise hub is to allow the applications to be directed to either the API Gateway or the IPaaS integrator while still maintaining the control on the requesting platform of standards to be used by the vendor. Figure 6 illustrates the logical view of this part of the model.

## 4. Validation by Use Case

This research validates a number of use cases against the developed architectural model. A set of Cloud Computing Use Cases at www.cloudsusecases.org has been put out by the Cloud computing Use Case Discussion Group. Three of the key use cases stated this discussion group are:

- End user to cloud,
- Enterprise to cloud to end user,
- Enterprise to cloud to enterprise.

Based on the above, the research uses workflow charts to validate the following examples of the above

listed use cases against the developed model:

- End user to the cloud e.g. accessing email;
- Enterprise to Cloud to End user e.g. publishing updates on the user desktops; and
- Enterprise to Cloud to Enterprise e.g. Down loading a report from a Supply Chain System.

## 4.1. Validation of the Use Case: Accessing Email

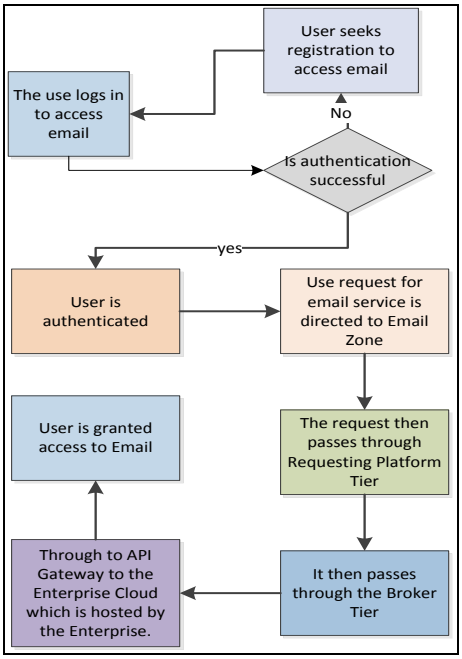


Fig. 7(a). End user to the cloud e.g. accessing email.

The diagram (Fig. 7(a)) illustrates how an end user is able to access an email from cloud, using the model

**Requirements for this use case**

The authentication service must be registered as a service being delivered by the enterprise private cloud.

The user must be registered to have access to the email service.

All architecture components must be working such as the email zone, the requesting platform and the broker tier to enable the successful transmission of the request and the response.

## 4.2. End-User to Cloud to End User e.g. Publishing Updates on the User Desktops

The Fig. 7(b) illustrates how an end user is able to access an email from cloud, using the model

**Requirements for this use case**

The user must be registered to request for this service.

The service must be registered in the Service Registry and in the SLA.

All architecture components must be working such as the email zone, the requesting platform and the broker tier to enable the successful transmission of the request and the response.

## 4.3. Enterprise to Cloud to Enterprise e.g. Downloading a Supply Chain Report: A Pre-set Service

The diagram (Fig. 7(c)) illustrates how an end user is able to download a supply chain report – a present service

**Requirements for this use case**

The system is set up correctly to trigger the download.

The service must be registered in the Service Registry and in the SLA.

All architecture components must be working such as the email zone, the requesting platform and the broker tier to enable the successful transmission of the request and the response.

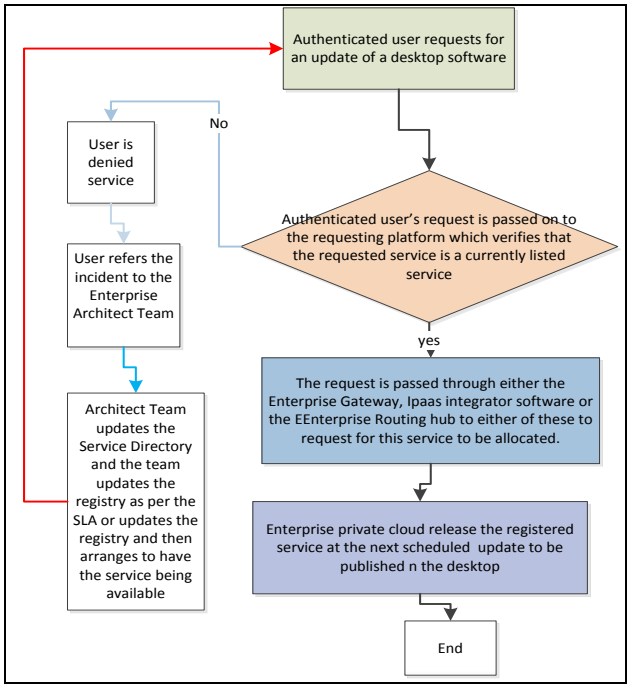


Fig. 7(b). Enterprise to cloud to end user e.g. publishing updates on the user desktops.

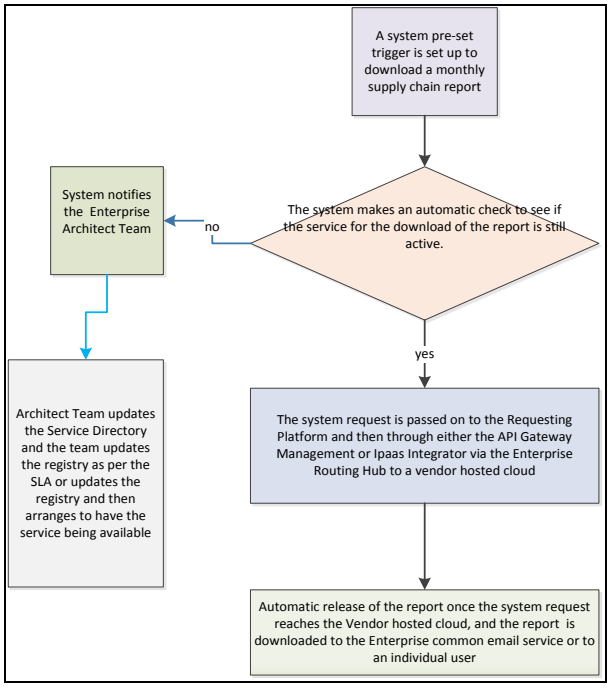


Fig. 7(c). Enterprise to cloud to enterprise e.g. downloading a supply chain report: A pre-set service.

## 5. Conclusions: Summary of the Model Based Architectural Model for the Enterprise Connection to Cloud Services

Current industry solutions via an API Management Gateway and or via the use of IPass Integrators do not provide a solution for the interoperability within an enterprise.

Hence the gap identified earlier that there is no proven academic literature to resolve the lack of seamless interoperability of cloud has been resolved. In revisiting the stated problem, this model validates the interoperation between EA and SOA to connect to cloud either via API Gateway, IPaas Integrator; or both API and IPaas Integrator . As such, this proposed researched model puts forth an architectural model that allows for the validation of the convergence of the three domains, namely EA, SOA and the Cloud Services. Hence, the research architectural model caters and supports the interoperation between EA and SAO; SOA and Cloud computing and the convergence of the above three.

Until further testing is carried out via use cases, it will be difficult to establish the cost of the provision of these services via this model. Thus this researched architectural model also provides an opportunity to the research community to validate their respective applications use cases and provide comments and feedback to the authors.

## References

[1] Sutherland, S. (2013). Convergence of interoperability of cloud computing, service oriented architecture and enterprise architecture. *International Journal of E-Entrepreneurship and Innovation, 4(1),* 43-51

[2] Tang, L., Dong, J., Zhao, Y., & Zhang, L. J. (2010, July). Enterprise cloud service architecture. *Proceedings of 2010 IEEE 3rd International Conference on Cloud Computing* (pp. 27-34).

[3] Wei, Y., & Brian, B. M. (2010). Service-oriented computing and cloud computing: Challenges and

opportunities. *IEEE Internet Computing, 14(6)*, 72-75.

[4] Raj, P., & Periasamy, M. (2011). The convergence of enterprise architecture (EA) and cloud computing. *Cloud Computing for Enterprise Architectures*, 61-87. Springer London.

[5] Sutherland, S. (2014). Secure APIs and protocols to connect enterprise applications to cloud services. *Proceedings of Informing Science & IT Education Conference* (pp. 323-336).

[6] Sutherland, S., & Chetty, G. (2014). Migration to cloud computing: a sample survey based on a research in progress on the investigation of standard based interoperability protocols for the convergence of cloud computing, service oriented architecture and enterprise architecture. *Int. J. Inf. Process. Manag, 5(1),* 50-61.

[7] Lewis, G. A. (2013, January). Role of standards in cloud-computing interoperability. *Proceedings of 2013 46th Hawaii International Conference on System Sciences* (pp. 1652-1661).

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

[9] The NIST definition of cloud computing (draft). NIST special publication 800: 145.

[10] Blatzan, P., Lynch, K., & Blakely, P. (2010). *Business Driven Information Systems*. McGraw Hill Australia Pty Ltd.

**Susan Sutherland** has post graduate qualifications in IS., business administration and education. She has worked in large and complex enterprises both public and private. Her experience includes operational and at strategic levels and has worked on the mainframe, midrange and desktop applications systems; and infrastructure and networks. Her infrastructure and network experience includes implementations of X.500, X400 and X435 standards. She has also consulted in migrating applications to Web 2.0. She was part of a team that implemented an internet security gateway service for a large government department. She had pioneered the deployment of the internet in the Australian government. She is interested in the deployment of bleeding edge technologies and their migration and integration into mainstream computing. Hence her motivation to undertake this research study in cloud computing interoperability is a natural progression of her previous work.

**Girija Chetty** has bachelor and master degrees in electrical engineering and computer science from India, and PhD in information sciences and engineering, from University of Canberra Australia.

She has more than 25 years of experience in Industry, Research and Teaching from Universities and Research and Development Organizations from India and Australia, and has held several leadership positions including head of Software Engineering and Computer Science, and course director for Master of Computing (Mainframe) Course. Currently, she is an associate professor, and the head of the Multimodal Systems and Information Fusion Group in University of Canberra, Australia, and leads a research group with several PhD students, Post Docs, research assistants and regular international and national visiting researchers.

Dr. Chetty is a senior member of IEEE, USA, and senior member of Australian Computer Society, and her research interests are in the area of multimodal systems, computer vision, pattern recognition, data mining, and medical image computing. She has published extensively with more than 140 fully refereed publications in several invited book chapters, edited books, high quality conference and journals, and she is in the editorial boards, technical review committees and regular reviewer for several IEEE, Elsevier and IET journals in the area related to her research interests.