Future SDP through Cloud Architectures

Foteini Andriopoulou and Dimitrios Lymberopoulos

Wire Communications Laboratory, Electrical and Computer Engineering Department, University of Patras, University Campus, 265 04 Rio Patras, Greece
{fandriop, dlympero}@upatras.gr

Abstract. In this paper we propose a new service delivery platform (SDP), named Future SDP that incorporates principles of cloud computing and service oriented architecture (SOA). Future SDP allows resources, services and middleware infrastructure deployed in diverse clouds to be delivered to users through a common cloud Broker. This cloud Broker is enhanced with policy, management, security and mediation functionalities that ensures proper use of development tools, resources and services only to certified participants of the federated clouds. This work focuses on solving interoperability problems both into infrastructure and middleware layer of the conventional SDPs. Finally, the operational attributes of Future SDP are depicted through a delivery scenario of healthcare telemonitoring services.

Keywords: SDP, Future SDP, cloud computing, hybrid cloud, federated cloud, cloud Broker, interoperability, integration, healthcare virtual "enterprise".

1 Introduction

In the last few decades, health information systems play a significant role in supporting patients and professionals and in improving the quality of healthcare. Healthcare systems rapidly moveded from treating isolated episodes towards a continuous treatment process involving multiple healthcare professionals and various healthcare infrastructures (e.g. hospitals, clinics, institutes).This rapid change in the healthcare domain imposes new demands on IT providers and motivates integration and interoperability between heterogeneous software components within the health information systems [1]. Integration and interoperability of different, heterogeneous software components, however, is a difficult task, as applications usually are vendor proprietary and not designed to cooperate with other vendor applications. Today powerful integration tools (e.g. application servers, object brokers, different kinds of message-oriented middleware, service delivery platforms - SDPs, etc) are available to overcome the heterogeneity of system components [2].

Nowadays, several industry organizations and standard bodies, such as OMA, TMF, 3GPP, IETF, the Parlay Group, SIP Forum, and others, have highly contributed to the evolution of SDP. Today's the third generation SDP is built around the primitives of Service Oriented Architecture (SOA) which enable efficient service integration, orchestration and lifecycle management [2, 3]. H. Lu et al in [4, 5] have already proposed a conceptual model for a next generation SDP (NG-SDP) where services will be automatically activated, without any manual interventions, evaluating user's contextual information. Nevertheless, for the eHealth domain the research efforts for the deployment of cognitive and autonomous SDPs are few. In [6] we proposed a NG-SDP for eHealth domain based on autonomous mentality enhanced with intelligent and cognitive functionalities. Despite the fact that is a well defined interoperable and autonomous platform, it is still a heavyweight software system.

Moreover, in the healthcare domain there is a revolution going on driven by the explosion in the ability to use modern communication infrastructures in medicine and the ubiquitous provisioning of healthcare services. Cloud Computing is a new paradigm that enables the patient's data collection in Healthcare institutions [7]. Also, efforts have been done in the development of EHR Systems based on cloud features [8, 9].

In this paper, we propose a SDP named Future SDP which is enhanced with cloud computing principles such as on-demand self- service and rapid elasticity. The new enhanced SDP will fully take advantage of the two technological innovations of SDP and cloud computing. Future SDP is expected to be widely accepted by enterprises and organizations since it will improve the quality of healthcare services and user experience, decrease the total costs since user pays only for the used services and provide seamless integration and interoperability in the healthcare environment. The Future SDP will be implemented by temporary federated clouds. The interoperability and integration functionality is

provided through horizontal cloud architecture established by the cloud Broker. This cloud Broker acts as an arbitrator and ensures the mediation, security, policy and management functionalities.

2 From SDP to the Future SDP

The novel SDP architecture has focused on the IT infrastructure which provides the interface and delivery machinery for the delivery and management of the service environment. However, the need for a new end-to-end architecture demands an advanced SDP in which boundaries between IT and network environments should be merged. This advanced SDP aims to span the complete service delivery environment.

2.1 Definition and architecture of SDP

According to the definition proposed in [2, 3, and 6], Service Delivery Platform (SDP) is a middleware architecture or environment that enables the efficient creation, deployment, execution, orchestration and management of one or more classes of services. Figure 1 demonstrates the abstract structure of SDP. The Enablers are deployed by Next Generation Network (NGN) or legacy telecommunication operators in order to facilitate the development of end user services, either internally within their organization, or external to 3rd party providers. All Enablers are implemented as building blocks of reusable services. Special APIs allow seamless access to these enablers by multiple end-users and 3rd party applications and services. Each Enabler implements a Publish/ Subscribe interface which allows an identified provider to receive information, events and inferences about a user. Message Broker in the enterprise domain is well known as Enterprise Service Bus (ESB). ESB is the appropriate messaging environment for efficient and consistent exchange of information / notifications or for session establishment among applications and enablers. Service Registry (SR) is the main store of the system that includes the services, applications and other information, which are delivered through the SDP. Service creation and execution environment contains the appropriate tools and facilities for the creation (orchestration and integration), modification and execution of the delivered services. Service Broker utilizes policies for the proper finding / discovering (from the SR), binding and invoking of the required services. Policy (PEEM) and Identity Enabler are responsible for the security and management of the system [2, 6].

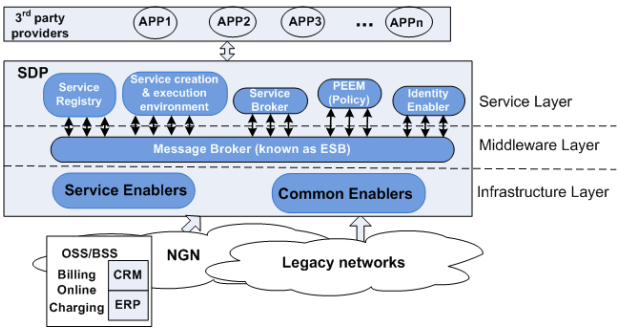

Fig. 1: The abstract structure of SDP.

2.2 Reasons for the transition from SDP to Future SDP

Even though SDP is not a well defined and standardized e-commerce environment, Moriana Group [3] insists that: “a service platform that uses vendor-specific software and hardware components; has network-specific, ‘vertical’ architecture; applies proprietary protocols and interfaces; requires special tools for service creation; or requires service and user data to be stored in an embedded database, falls into the ‘stove pipe’ category and should not be called an SDP”.

The current commercial implementations and research results are strictly depended upon proprietary “lock-in” vendor software and hardware components. The dependence of such specific

vendor components creates interoperability and openness problems, similar to the problems yielded by all vertical architectures.

In this paper we introduce the notion of the "Future" SDP that considers many-to-many relationship between different vendor software and hardware components. Moreover, Future SDP provides not only an environment for delivery and management services but also provides a service creation, deployment and execution environment. The Future SDP tends to solve interoperability problems and establish horizontal architectures through the involved components of the SDP.

In the market field [10], the reasons that demand transition from SDP to Future SDP are:

1. Communication Service Providers (CSPs) require more openness, extendibility and flexibility from service platforms to quickly boost their service delivery capabilities. New customized services (e.g. VoIP, IPTV, VoD, mobile commerce, mobile banking, mobile payment, mobile advertising) are upcoming.
2. Mobile Network Operators (MNOs) try to find new ways so as to increase the average revenue per user through attractive mobile content and advertising, as well as service bundling and advanced services to their prepaid customer base.
3. Ongoing network convergence enables core voice services to be transferred across legacy and IP networks. SDP's integration and interoperability supports convergent charging and billing for mobile, fixed, broadband, IPTV and other service categories. The traditional distinction between pre-paid and post-paid subscribers is removed. Also, SDP migrates broadband services, convergence of lines of business and customer experience oriented management adoption via the OSS/BSS infrastructure.
4. The adaptation of new business models in order to create new revenue streams and sustainable competitive strategies

3 Future SDP

3.1 Definition and Characteristics

SDP is characterized as Future SDP whenever it is constructed by reusable open software and hardware components and whenever it applies standard protocols and interfaces [3]. Following, the five key characteristics of the Future SDP middleware architecture are analyzed:

Open service creation environment: The SDP development architecture must be open, in order to enable the creation of new services and applications with the usage of various open development tools (e.g. Eclipse or MS Visual Studio), open interfaces (e.g. Application Programming Interface – APIs) as well as a common set of service components (e.g. email, VoIP, etc). Irrespectively to the creation environment, the created new services have to be executed efficiently in any execution environment using open APIs and Web Services.

Common service execution environment: The SDP execution architecture must consist of a number of common components, such as service enablers, the service and user profile repository, service orchestration and management mechanisms, as well as common OSS/BSS interfaces for charging and provisioning.

Standardized technology: Both service creation and execution environments should be based on open IT and telecom standards (e.g. middleware, protocols, APIs, service enablers, service execution models, service creation tools (SDKs) and data repositories).

Horizontal architecture: The SDP architecture should dynamically provide integration and interoperability (interactions) between different networks (wireless, broadband, IMS, NGN, etc.). It consists of clearly defined functional layers for service execution, integration and exposure. It should also provide secure access to network capabilities through a set of abstracted service enablers rather than through native protocols.

SOA-based integration: It is based on the principles of Service Oriented Architecture (SOA) for purposes of integration between services and functionalities of Operation and Business Support System (OSS/BSS) as well as the service's management and orchestration.

3.2 Architecture of the proposed Future SDP

Fig. 2 depicts the architecture of the proposed Future SDP that is based on cloud computing principles. In comparison to the conventional SDP architecture of Fig.1: (a) the middleware and service layers are replaced with a cloud Broker, (b) the service enablers as well as the services and applications provided by 3rd party providers, in the Future SDP are resources and services hosted in the deployed private cloud infrastructures and (c) the common enablers are hosted resources and services deployed upon any public cloud infrastructures. All the involved clouds compose a hybrid cloud that is maintained by the cloud Broker.

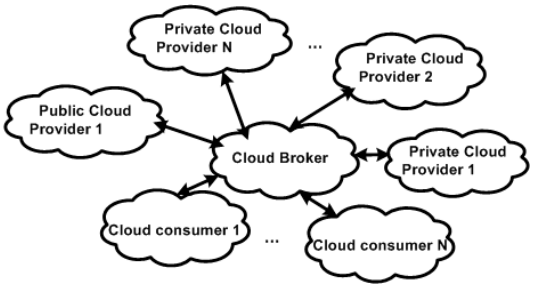

Fig. 2: The overview of the hybrid cloud

This hybrid cloud is a cloud infrastructure which is composed of two or more clouds (private, community, or public), where each cloud remains unique and all clouds are bound together through a cloud Broker that enables data and application portability (e.g. cloud bursting for load-balancing between clouds). Through Broker, instances of all clouds (composing the hybrid cloud) can communicate with each other. Moreover, the Broker ensures the interoperable interaction among all the entities (users and applications) that are deployed upon the hybrid cloud.

The cloud Broker is the central component of the proposed Future SDP architecture. It provides integration between resources and services from multiple heterogeneous cloud providers and interacts on-demand and transparent with the cloud consumers in order to satisfy their requests. The Broker contains a catalogue where each cloud provider advertises or publishes resources and services that he is willing to share with or rent to the other clouds. Moreover, resources and services are not hosted permanently in the Broker, but are dynamically provisioned from collaborative private and public clouds.

In each consumer's request for provisioning of services, the cloud Broker establishes a temporary federated cloud (Fig. 3) [11, 12]. Federated cloud is a collaboration of cloud providers that rent resources or deliver services to the cloud Broker in order to satisfy this consumer's request. In order to provide dynamically integration and interoperability (interactions) within the federated cloud, the horizontal deployment of the involved resources has to be established through the cloud Broker.

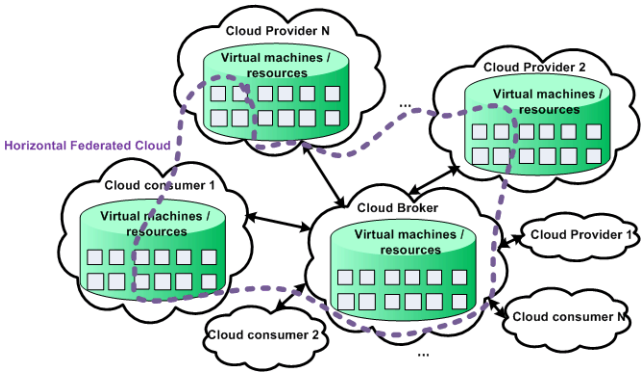

Fig. 3: An overview of the established federated cloud.

3.3 Architecture of the proposed Cloud Broker

Cloud Broker provider creates a cloud platform/environment so as to simplify the delivery of complex services and resources with different syntactic and semantic ontologies to cloud customers

[12, 13]. Also, Cloud Broker negotiates and handles policies and Service Level Agreements (SLAs) between cloud providers and cloud consumers or through cooperative cloud providers in the federated cloud.

The Cloud Broker is composed of the following key components (Fig. 4):

I. *Resource Registry:* It is a database where each cloud provider has published his own catalogue with services and resources which provides for being easily accessed by the Broker.

II. *Creation and Execution Environment (CEE):* It provides access to a wide variety of proprietary or rent facilities (e.g. virtual machines, physical computers, business logic languages - BPELs, libraries, interfaces - APIs, compilers and development tools). Through CEE, federated providers and users can integrate resources and services so as to customize the appropriate services with their targets. Moreover, CEE can start a virtual machine either for direct execution of application or for content storage and usage.

III. *Mediator:* It is responsible to control which resources and from which cloud provider will be used. Moreover, it negotiates the policies and the SLAs that will be executed per case. Actually, Mediator has the role of an enhanced message broker (a combination of the message and service broker in Fig. 1) with management and security functionality for the establishment of horizontal federated clouds.

IV. *Policy Handler:* It contains a repository with all the SLAs published by cloud providers. Whenever a consumer requires services or resources, the Mediator negotiates and matches the consumer's SLA requirements with the services each cloud provider offers and then Policy Handler finds the most appropriate matching.

V. *Identity Manager*: It verifies cloud providers and consumers in order to prevent malicious and unauthorized access into cloud resources and services. Moreover, it generates and provides a single-sing-on ticket for consumers and providers to have unlimited access without the need to be authenticated and authorized again and again in all phases until the request satisfaction.

VI. *Security Handler*: It blocks malicious traffic to and from various components exposed by the interfaces of the cloud Broker service. It manages the overall security of the Broker's platform. It cooperates with Identity Manager and Policy Handler in order to prevent unauthorized access, modification or denial of network infrastructure facilities and resources. Furthermore, firewalls are used for the detection of intrusions focusing on protecting data, resources and services from malware, virus, worms, or Trojans.

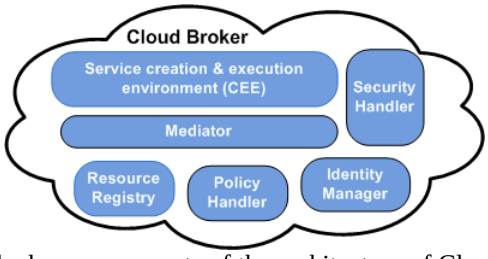

Fig. 4: The key components of the architecture of Cloud Broker

3.4 How the proposed architecture achieves the main characteristics of the Future SDP.

The key characteristics in the proposed architecture of the Future SDP (section 3.1) are achieved as follows:

Open service creation environment: The establishment of Future SDP with the principles of cloud computing provides the openness that is demanded. All the cloud providers publish in the cloud Broker (in Resource Registry) their resources (data, virtual machines, development tools, APIs, etc) in order to be accessed from Broker and provide (deliver or rent) their services. Specifically, the open creation environment is implemented through the CCE component of the cloud Broker. CEE contains a repository with all the development tools, APIs and service components that all the providers offer. CEE provides the open creation that is demanded in a Future SDP in order to integrate resources within a federated cloud. Through the resource integration new services are created and executed in the CEE.

Common service execution environment: The Future SDP is composed of virtual resources and machines that are hosted in the cloud Broker or rent from cloud providers for the purposes of management, charging and provisioning. The execution environment is implemented in the federated cloud and Broker is the handler of the execution process. According to this manner, CEE component

executes processes and the response to these processes is sent through the Mediator to the cloud provider or consumer that has started the procedure

Standardized technology: The above analyzed open character of the proposed Future SDP is strongly coupled with the necessity of using standardized technology in all components, middleware, protocols, APIs, service enablers, service execution models, service creation tools (SDKs) and data repositories.

Horizontal architecture: The Future SDP architecture should dynamically provide integration and interoperability between different networks (wireless, broadband, IMS, NGN, etc.). The horizontal architecture is achieved through the federations between heterogeneous clouds. Cloud Broker is the central component that is acting as mediator, integrator and manager so as to solve interoperable problems in all the layers (service, middleware and infrastructure). Specifically, the interoperability problem in all these layers is handled through Resource Registry and CEE components that contain repositories with libraries for APIs, BPELs, ontologies, etc.

SOA-based integration: According to NIST, all cloud infrastructures are based upon the principles of SOA [14]. Moreover, in the architecture of Broker, the Mediator implements the principles of SOA [2,3] through the integration of Operation and Business Support System (OSS/BSS) with services and the functionality of CEE, as well as the functionalities of management and orchestration are based on SOA.

4 The proposed Future SDP in the healthcare domain

The proposed Future SDP for the healthcare domain consists of: (a) a cloud consumer (user) who needs external resources and services; (b) many cloud providers who offer / rent their resources or services or both of them in a seamless manner and (c) a cloud Broker provider who acts as a message broker, a mediator, integrator and manager. The Broker is responsible for the negotiation and transformation of the required resources or services.

4.1 Architecture of the proposed Future SDP

The overall architecture of the proposed Future SDP for healthcare purposes is composed of the following units (Fig. 5):

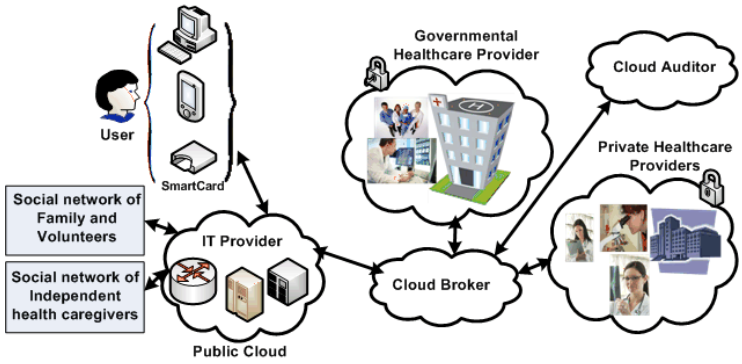

Fig. 5: The architecture of the proposed Healthcare system.

1) *Governmental Healthcare Provider (GHP)*: It is built upon a community cloud infrastructure where several governmental organizations (e.g. hospitals, clinics, pharmacies, insurance companies, etc.) jointly construct and share the same cloud infrastructure as well as policies, requirements, values, and properties. In GHP a variety of caregivers (doctors, nurses, ambulance service, etc) is hosted for monitoring patients. The different health units (domains) cooperate with each other to form a Circle of Trust (CoT) where each unit keeps a registry of trustworthy services provided by other units (e.g. doctors with laboratory domain). Functionally GHP performs dual roles, either as an individual entity (e.g. 3rd party cloud provider with applications and services ready for use Fig. 1) or as Service Enabler that provides an aggregation of enablers (e.g. resources and services in Fig.1).

2) *Private Healthcare Providers (PHP)*: They are built upon private cloud infrastructures. Each PHP has its own infrastructure where virtual machines and resources are hosted to provide services to their clients in order to connect caregivers or EHR (Electronic Health Record) from different domains with the requestor of the service. Similarly to the GHP, PHP are deployed as Service Enabler ready for use or "resell".
3) *IT Provider:* It is built upon a public cloud and provides convenient, on-demand network access to a shared pool of configurable resources (e.g. networks, servers, storage, services, etc). The patient is a subscriber in the IT cloud provider which has the fully ownership of the cloud with its own policy, charging, profit, billing and monitoring models but it is provisioned for open use by the general public. The public cloud supports the public cloud consumers (social network of family and volunteers) as well as cloud providers (social network of independent caregivers). In this case the IT provider is represented as Common Enabler so as to add communications features.
4) *Cloud Broker:* is responsible for the management, performance and delivery of cloud services and negotiates the policies and rules between cloud consumers and cloud providers for the appropriate delivery of the services. The major services provided by the cloud Broker are aligned with the NIST Cloud Computing Reference Architecture [14] and they include:
    - *Service Intermediation:* Broker enhances a given service by improving some specific capability and providing value-added services to cloud consumers. The improvement can manage access to cloud services, identity management, performance reporting, enhanced security, etc.
    - *Service Aggregation:* Broker combines and integrates multiple services into one or more new services. It provides data integration and ensures the secure data portability between cloud consumers and multiple providers.
    - *Service Arbitrage*: Broker has the flexibility to choose between fixed and not fixed services from multiple providers.
5) *Cloud Auditor:* It is a third party cloud provider that conducts an independent audit of the cloud services, information system operations and determines the security of the cloud implementation. An auditor is essential for the evaluation of services provided by cloud providers [14].
6) *User:* It is the consumer (e.g. patient, doctor, nurse, etc.) of the services or resources provided by cloud providers. The secure access and process of user's personal data, composed in form of personal profile and EHR, is achieved through : (a) Single Sign-On (SSO) authentication, a cloud consumer should be able to authenticate itself once, gaining access to the resources provided by the federated cloud belonging to the same trust context, without further identity checks; (b) digital identities by third parties, each cloud consumer should be able to authenticate itself with the foreign clouds using its digital identity guaranteed by a third party provider.

5 Implementation of the Future SDP in healthcare domain

In this section we demonstrate the operational attributes of the proposed Future SDP through a real world healthcare scenario. We consider the case where a user (patient) demands to establish a videoconferencing session with a doctor because he feels intense pain in the chest and cannot breathe easily. In this scenario a federated cloud is established between the user, IT Provider, cloud Broker and Healthcare Providers. The cloud Broker supports the overall caregiving process through two discrete phases: a) the integration of all required resources (medical, operational, context, etc) in order to create the current instance of the user's profile (depicted in Fig. 6), and b) the deployment of the appropriate environment for the execution of the required telemonitoring tasks, such as medical examinations by means of virtual machines (depicted in Fig. 7).

It should be mentioned that in both phases, cloud Broker should perform: (a) authentication so as to establish a trust circle with the involved clouds in the federated cloud; (b) discovering and binding of services and resources (e.g. user's EHR and profile, sensor measurements, etc) from different cloud providers; and (c) establishing a virtual enterprise / environment either to integrate resources (integration phase) or to execute a service or process that (patient or doctor) cannot handle (execution phase). In the integration phase, interoperability should be achieved in the infrastructure layer while in the execution phase interoperability should be achieved in the middleware layer.

A. Integration Phase

We consider that whenever a cloud provider joins the hybrid healthcare cloud it publishes into the Resource Registry of cloud Broker the services and resources that the cloud provider is willing to rent (share) and provide.

Step A.1 (Authentication of user and IT Provider): The cloud Broker (through Identity Manager) has the responsibility to control if the user (patient) is authenticated to accept telemonitoring services by the healthcare cloud providers of the hybrid cloud. If the user is authenticated then cloud Broker authorizes the IT provider with the capability to establish videoconference sessions between the user and the medical personnel of the healthcare cloud providers

Step A.2 (Discovery of the required service): The IT provider pushes the user's requests, id and password to the cloud Broker (Mediator) and demands to find all doctors that are located in the user's neighborhood and are with on-line status (discovery of service).

Step A.3 (Binding of the required service): Mediator: (a) checks the Resource Registry in order to find and bind the healthcare cloud providers (hospitals, clinics or individuals) that provide healthcare service by activating healthcare professionals that are available for treating patient (user); (b) interacts with the Policy Handler to negotiate and finally find and bind the appropriate cloud provider according to the user's SLA's, QoS and policies. The selected healthcare cloud provider, the cloud Broker and the IT provider establish the federated cloud.

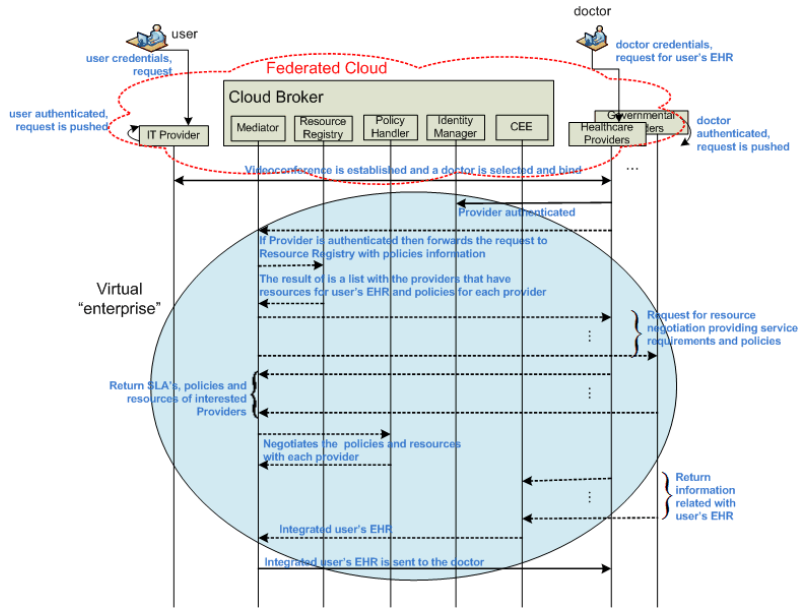

Fig. 6: The sequence diagram of Storage context

During the above three steps, we have created a federated cloud where the cloud Broker acts as a conventional message broker (handling messages yielded by the involved providers) enhanced with functionality for the negotiation and sharing of the provided resources by any involved provider (policy determination). The following three steps (A.4 to A.6) describe the way the federated cloud operates for the above mentioned healthcare scenario for integrating resources from the involved providers in the federation. Within the federated cloud, the healthcare providers as well as the IT provider rent to the cloud Broker their resources (e.g. Lab exams, medication, user's profile, etc) for the creation of the total EHR of the user. Hence, during the integration process, a "*virtual enterprise*" is progressively established between the involved entities of the federated cloud.

Step A.4 (Discovery & binding of the required resources): Since the videoconference between user and doctor is established, the doctor requests the total user's EHR. We consider that the total EHR is composed of various items (e.g. examinations) that are dispersed (hosted) in many private and public clouds (e.g. hospital, private labs, clinics, social network of individual doctors, etc). This step has the responsibility: a) to discover all the clouds that contain items of the EHR and b) to bind all these clouds into the current federation cloud. The Policy Handler negotiates the policies for the above binding.

Step A.5 (Integration of EHR resources): CEE of the cloud Broker creates a temporary virtual EHR that is visible and accessible by the requestor or by other authorized entities (e,g, doctors) within the trust circle of the federated cloud. Hence, doctor has a completely knowledge (information) about user's profile (user's history, lab exams, medication, etc) and can treat user.

Step A.6 (Release of the federated cloud): After the release of the videoconference, the federation of the clouds is released.

B. Execution Phase

We consider that during the videoconference session, the doctor evaluates the medical situation of the user (patient). For instance, biodata could be acquired in real time by the tele-monitoring system. We consider the case where the user is not supported by sensors or devices (e.g. spirometer, real-time vital signs monitor, electrocardiograph, etc) appropriate for the collection of those biodata that are related with his current medical episode. In this case, the doctor determines the appropriate sensor device (for the provision of the biodata) and requests from Mediator to find and bind the most suitable healthcare cloud provider for this request. Hence, the existed federated cloud is expanded with new cloud providers that support the secure acquisition of biodata (virtual enterprise / environment).

Step B.1 (Authentication of user and IT Provider), B. 2 (Discovery of the required service) and B.3 (Binding of the required service) are similar to steps A.1 to A.3.

Step B.4 (Discovery & binding of the required middleware): Since the videoconference session between doctor and patient is established, then, the doctor requests from Broker to provide to the user an electrocardiograph virtual machine. The Mediator finds and binds a cloud provider that has the appropriate virtual machine from Resources Registry. Through Policy Handler, the Mediator negotiates policies and SLA's with the cloud provider and then provides a CEE for integration and execution.

Step B.5 (Execution of the appropriate virtual machine): In this virtual environment the Broker acts as a middleware and an arbitrator between user and doctor. Through Broker, Virtualization Machine Monitors (VMMs) (i.e. virtual machines) are provided to the user. VMMs run "guest" software (e.g. middleware) executed as if it was installed on a stand-alone hardware platform. Moreover, the Broker provides the execution environment (CEE) for executing the middleware such as virtual exams and the result is forwarded to the doctor.

Step B.6 (Release of the federated cloud): After the forwarding of the results, if the doctor requests to integrate this result with user's exam and EHR the steps A.4 to A.6 should be repeated, otherwise, with the release of the videoconference, the federation of the clouds is released.

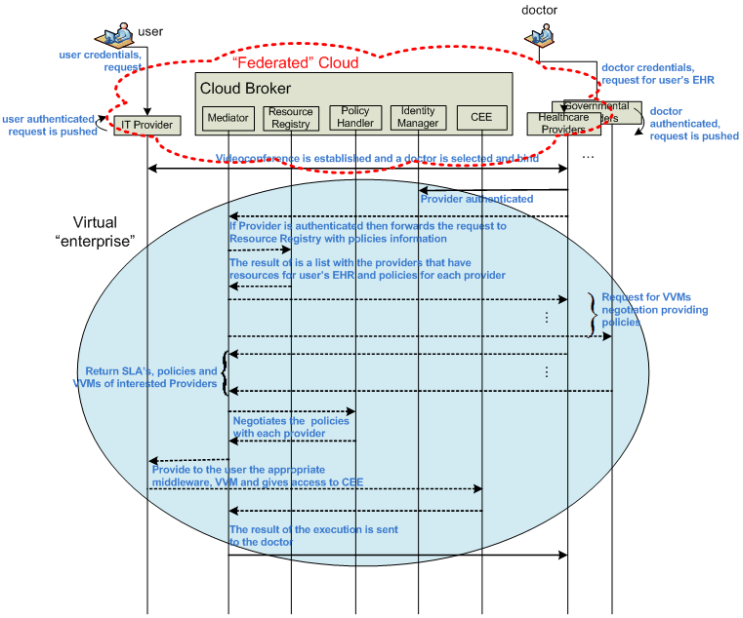

Fig. 7: The sequence diagram of Execution Context.

With these processes, the doctor has a complete image of the patient's vital signs often skipping intermediate steps and caregivers (e.g. request from user to visit an emergency department or a clinic).

6 Conclusion and Future Work

This paper proposes a way to relate SDP and cloud computing in order to establish an open and seamless SDP architecture, named Future SDP. Incorporating conventional SDP's features into cloud

computing principles enables Future SDP to integrate and deliver data and services hosted to any private and public clouds. This innovation establishes an horizontal SDP architecture that can minimize the interoperability problems of the existing vertical / proprietary SDP architectures. The central component of this architecture is the Cloud Broker that handles the efficient process of users' requests and the effective provisioning of data and services hosted within any federated cloud scheme. Since interoperability is achieved, SDP and cloud computing can take advantage of all benefits provided to both SDP and cloud.

Finally, in order to clarify the potential role of the Broker in the architecture, we described through sequence diagrams the implementation of a simple healthcare scenario using the Cloud Broker in two different phases of integration and execution.

In the real world there are numerous products of cloud infrastructures. Our main goal is to achieve interoperable interaction through a cloud Broker between different products (e.g. OpenNebula and Microsoft Azure platform). We plan to study the performance of such a Future SDP, evaluating the components behavior and employing a simulated environment. This environment will be consisted of more than ten clouds dynamically joining and leaving federations.

References

1 Continua Health Alliance, http://www.continuaalliance.org/index.html

2 F. Andriopoulou, and D. Lymberopoulos, "A new platform for delivery interoperable Telemedicine services," in Proc. Second Int. ICST Conf on Wireless Mobile Communication and Healthcare, pp.181-188, October 5-7, Kos Island, 2011.

3 Moriana Group, Service Delivery Platforms – definition and evolution, November 2011, http://www.morianagroup.com/index.php?option=com_content&view=article&id=148&Itemid=233

4 H. Lu, Y. Zheng and Y. Sun, "The Next Generation SDP Architecture: Based on SOA and Integrated with IMS," in Proc. Second Intern. Symp. on Intelligent Information Technology Application, pp. 141 – 145, December 20-22, 2008.

5 Y. Zheng, H. Lu, and Y. Sun, "A Cognitive SDP Model: A telecom way to help social computing in communications and interactions," in Proc. Intern. Symp. on Knowledge Acquisition and Modeling, pp. 572 – 575, December 21-22, 2008.

6 F. Andriopoulou, N. Lazarou, and D. Lymperopoulos, "A proposed Next Generation Service Delivery Platform (NG-SDP) for eHealth domain," in Proc. of 34th Annual Intern. Conf. of the IEEE Engineering in Medicine and Biology Society, August 28- September 1, San Diego, 2012.

7 C. Rolim, F. Koch, C. Westphall, J. Werner, A. Fracalossi, and G. Salvador, "A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions," in Proc. of Second International Conference on eHealth, Telemedicine, and Social Medicine, pp. 95-99, February 10-16, 2010

8 Y. Chen, J. Lu, and J. Jan, , "A Secure HER System Based on Hybrid clouds," Journal of Medical Systems, 2012.

9 S. Kikuchi, S. Sachdeva, and S. Bhalla, "Applying Cloud Computing Model in PHR Architecture," in Proc. of the Joint International Conference on Human-Centered Computer Environments, pp. 236-237, 2012.

10 Moriana Group, Market Studies and Forecasts - SDP Market Analysis 2009-2012.

11 A. Celesti, F. Tusa, et al, How to Enhance Cloud Architectures to Enable Cross-Federation, 3rd International Conference on Cloud Computing(CLOUD), IEEE 2010, pp. 337 – 345.

12 R. Buyya, R. Ranjan and R. N. Calheiros, "InterCloud: Utility – Oriented Federation of Cloud Computing Environments for Scaling of Application Services," LNCS Algorithms and Architectures for Parallel Processing, vol. 6081, pp. 13-31, 2010.

13 S. Grivas, Tr. Kumar, and H. Wache, "Cloud Broker: Bringing Intelligence into the Cloud / An Event-Based Approach," in Proc. of 3rd Intern. Conf. on Cloud Computing, pp. 544- 545, July 5-10, 2010

14 R. Bohn, J. Messina, et al, NIST Cloud Computing Reference Architecture, NIST SP - 500-292, September 2011, pp. 1-35.