# Using a software architecture based on a Private Central Proxy Cloud to improve a Health Center System

Majda Elhozmari*, Ahmed Ettalbi**

*Models and Systems Engineering Team, SIME Laboratory ENSIAS,
University of Mohammed V Rabat, Morocco
*elhozmari.majda@gmail.com,
**ettalbi1000@gmail.com

**Résumé.** In Collaborative and secure sharing of healthcare data in multi-clouds, Fabian, Ermakova and, Junghanns realized a solution of a novel architecture that externalizes data and its implementation for inter-organizational data sharing, which provides a high level of security and privacy for patient data in semi-trusted cloud computing environments, using Multi-Cloud Proxy (MCP) by the side of Client. But one of the biggest challenges here is the recovery of stored data. For one request, MCP must search the data requested into different Cloud providers, which can bring some drawbacks like network overload and decrease the level of security. Therefore, the focus of our article is to propose a solution by using a Private Central Proxy Cloud implemented in a private Cloud environment, which can be an intermediate between different Cloud providers and health centers. All that to get benefits such as tight coupling, increasing the level of security, minimizing network overload problem and recovering data easily.

## 1 Introduction

Cloud Computing has been the IT hype of 2010. Behind this fuzzy term cover some many known concepts such as virtualization and outsourcing of data. During the last years, the offers of Cloud solutions were multiplied and proposed by most of major factors in the IT. Smaller actors also offer solutions in the Cloud by using sometimes hardware resources made available by the IT giants famous Clouds. Before Cloud Computing, traditional applications have always been very complicated and expensive. Nowadays Cloud Computing technology is much easier and quicker to integrate with enterprise applications. It can help to eliminate problems of managing hardware and software because the provider is the responsible for managing and maintaining Cloud infrastructure. Also Cloud gives the consumers what they need with low cost, upgrades are automatic and scaling up or down is easy. Cloud Computing offers business users the chance to immediately implement services with usage-based billing that are tailored to their requirements, often without the need to consult with the IT department. Hence, many business applications are moving to the Cloud ; for example, cloud based system in the health domain (Kaur et Chana, 2014). The Cloud exists in several forms : private Cloud when mutualizes company resources (through virtualization), public Cloud where data will be placed

directly at the supplier. Many legitimate concerns are raised in the public Cloud, but sometimes they are poorly targeted. We must not forget that security is a major issue for the service provider. Nowadays, it is a big challenge to guarantee the confidentiality of data in the Cloud. There is a classification of services that can be found in the Cloud. The most popular type of services is Software as a Service (SaaS), which is to make a web application available and ready for use directly as the payment has been confirmed. The popularity of these solutions comes from their very low cost of entry and rapid provision users. In addition, these solutions are generally less expensive than traditional applications and do not require technical personnel for maintenance. Also, the consumer is not forced to make updates. While it is easy to get into the Cloud, getting out is a delicate operation. The Cloud can be used without too much danger to meet a specific need ; it will probably be more effective and less expensive than a traditional solution. For long term use, various precautions should be taken under penalty of no longer control the evolution of costs. Anyway, the Cloud has many advantages and deserves to be exploiting : whether for small and medium business, large companies or the public sector, there are opportunities to be seized in the Cloud. In this paper, we focus on inter-organization sharing big data between different Cloud providers, especially in healthcare domain. For that, we studied architecture proposed by Fabian et al. (2015). In this paper, Fabian, Ermakova and Junghanns proposed a solution of a novel architecture that externalizes data and its implementation for inter-organizational data sharing. After studying, we stand out some challenges that we'll explain below. Also in this paper we will propose a global solution for controlling communication between both Cloud providers and MCP (Multi-Cloud Proxy) using a Private Central Proxy Cloud. This solution aims maximizing the level of security and minimizing interaction between MCP and Cloud providers. The remainder of this paper is organized as follows : Section Two presents the definition, characteristics, some benefits and drawbacks of SOA. Section Three defines Cloud Computing and explains different types of Cloud. Section Four explains the problematic of the paper between Cloud providers and MCP. In section Five, we propose an architecture that resolves the problem. We conclude this paper by presenting our further works.

# 2 Definition and characteristics of SOA

## 2.1 Definition of services

Services are the essential concept of SOA. There are not originally technical concepts. The idea of services was developed in the world of business. It consists of a well-defined function or feature. It is also a standalone component that is independent of any context or external service. It is divided into operations which constitute specific actions that the service can achieve. A service is a processing entity that meets the following characteristics :

- **Large granularity (coarse-grained) :** The proposed service operations encapsulate multiple functions and operate on a wide scope of data to the contrary, the concept of technical component ;
- **Interface :** A service can implement multiple interfaces, as well as several services can implement a common interface ;
- **Localizable :** Before calling (bind, invoke) service, you will find (find) ;

- **Single instance :** Unlike components that are instantiated on demand and can have multiple instances at the same time, a service is unique ;
- **Low coupling (loosely-coupled) :** Services are connected to customers and other services via standards. These standards ensure decoupling, that mean reducing dependencies. These standards are XML documents like web services.

The service concept makes also possible further features of SOA. These provide additional benefits.

## 2.2 Definition of SOA

Service Oriented Architecture is one of the most important enterprises IT system architecture. More than technology or method, it is a convergence of several existing approach. SOA is an emerging architectural style for developing and integrating enterprise systems information applications governed by business processes. SOA integrates these different practices in an organized framework to enable an enterprise to deliver self-describing and platform independent business functionality (Cartright et Doemenburg, 2006), strongly guided by the business. Indeed, too focused experiments on a single approach or guided by the technique did not provide satisfactory answers. SOA is essentially a collection of services supporting communication between each other. This makes it possible to introduce other ideas, such as service bus, service composition, and service virtualization. Each of them can be applied to the architecture of an enterprise to deliver benefits, such as :

- **Technological neutrality :** Ensure full independence between interfaces and implementations. The element that uses a service must not be forced nor by the implementation technology, nor by its location (potentially distributed) ;
- **Service Re-Use :** Promote reuse of business services through several business lines or applications and allow high-level building services by combining existing services ;
- **Front-End based unbiased combination :** The introductory web services standards use extensible Markup Language (XML), which is related to the establishment and use of enclosed content. Regardless of the development language used, these systems can provide and cite services through a familiar system (Goyal et Jain, 2012) ;
- **Versioning :** Like any element of software, service components are subject to changes (maintenance or functional changes). Pooling service has more or less significant impact on consumers of these services, depending on the type of evolution : the addition of a new interface or operation, the implementation of change (without modification of service interfaces), modification of existing interface, changing the types of data exchange ;
- **Dependence of interfaces :** Each service component may potentially expose several interfaces (which contain each of the service operations). The arm's length at the interfaces allows a finer understanding of the structure of the system and facilitates impact analysis.
- **Visibility of IT system :** The concept of perimeter visibility of a service is not a side issue and impacts the organization as well as architecture. It specifies the elements that have the right to use it as a consumer service ;
- **More security :** The creation of a service layer by definition means that developers have created an additional network interface that can be used by multiple applications. When systems were built using client-server methods, security is normally handled on the front-end ;

- **Better testing :** Whereas in the service component as a quick package from the viewpoint of service consumers, the test elements are involved parties in consumer specification. Services have published interfaces that can be tested easily by developers by writing unit tests. Developers can use tools such as JUnit for creating test suites. These test suites can be run to validate the service independently from any application that uses the service ;
- **Controlling pre-existing systems :** One general use of SOA is to classify essentials or function of in hand application systems and make them available to the enterprise in a traditional predetermined manner, controlling the extensive venture previously done in pre-existing applications (Goyal et Jain, 2012).

### 2.3 Limits of SOA

Although its benefits, SOA have some limits such as (Mahmood, 2007) :
- **Conflicts of interest :** There is a risk of conflict of interest between responsible for application projects and SOA objectives. The first is evaluated by their ability to deliver on time the corresponding elements to specifications within the established costs. The inclusion of transverse factors can be seen as an additional constraint. The role of management is fundamental to ensure the coordination and actions for effective collaboration with cross-functional teams ;
- **Vendor lock-ins :** Such as many architectures that are based on proprietary protocols and implementations ;
- **Tight coupling :** Such as distributed architectures typically link components directly to one another ;
- **Complexity :** The interactions between objects are often rich and complex ;
- **Connectivity :** Such as majority of distributed architectures, SOA does not work over wide-area, intermittent networks ;
- **Quality assurance :** this is particularly difficult as services are distributed and ownership is often unclear ;
- **WS standards :** These standards are open and amorphous. Many are still working drafts. Higher level services and security have not been standardized at all ;
- **Security :** When using open standards, a service is much more open to other services and applications than a monolithic application and thus security becomes an issue. Although WS-Security addresses such issues, there is a considerable amount of work that still needs to be done.

## 3 Definition and characteristics of Cloud Computing

### 3.1 Definition of Cloud Computing

National Institute of Standards and Technology (NIST) defines Cloud Computing as a model for allowing ubiquitous, convenient, on-demand network access to a shared pool of configurable computing that can be rapidly provisioned and released with minimal management effort or service provider interaction (Hogan et al., 2011). Cloud model is composed of five essential characteristics, three service models, and four deployment models (Hogan et al., 2011).

## 3.2 Essential Characteristics of Cloud Computing

- **On-demand self-service :** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- **Broad network access :** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, workstations).
- **Resource pooling :** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state or datacenter). Examples of resources include storage, processing, memory and network bandwidth.
- **Rapid elasticity :** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- **Measured service :** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both the provider and consumer of the service use.

## 3.3 Service Models

- **Software as a Service (SaaS) :** The capability provided to the consumer is to use the provider's applications running on a Cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email) or a program interface. The consumer does not manage or control the underlying Cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings ;
- **Platform as a Service (PaaS) :** The capability provided to the consumer is to deploy onto the Cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services and tools supported by the provider. The consumer does not manage or control the underlying Cloud infrastructure including network, servers, operating systems or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment ;
- **Infrastructure as a Service (IaaS) :** The capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying Cloud infrastructure but has control over operating systems, storage and deployed appli-

cations ; and possibly limited control of select networking components (e.g., host firewalls).

### 3.4 Service Models

- **Private Cloud :** The Cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed and operated by the organization, a third party, or some combination of them, and it may exist on or off premises ;
- **Community Cloud :** The Cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy and compliance considerations). It may be owned, managed and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises ;
- **Public Cloud :** The Cloud infrastructure is provisioned for open use by the general public. It may be owned, managed and operated by a business, academic, government organization, or some combination of them. It exists on the premises of the Cloud provider ;
- **Hybrid Cloud :** The Cloud infrastructure is a composition of two or more distinct Cloud infrastructures (private, community or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., Cloud bursting for load balancing between Clouds).

## 4 Problematic

Everyone talk about Cloud Computing. It is the last fashion of technologies registration, and on-demand network access to a shared pool of configurable computing, that can be rapidly provisioned and released with minimal management effort or service provider interaction. Before Cloud Computing, traditional business applications have always been very complicated and expensive, especially in data storage domain. Nowadays, Cloud Computing technology is much easier and quicker to integrate with enterprise applications. It can help to eliminate problems of managing hardware and software, because provider is the responsible of managing and maintaining Cloud infrastructure. Also Cloud gives to consumer what he needs with less cost, upgrades are automatic, and scaling up or down is easy. Cloud Computing offers business and organization users the chance of storing data, using Cloud Storage that provides possibility to store data with huge capability of adaptability with amount of data, by elasticity of storage area. Data stored in the cloud can be accessed from any place at any time. In that why, most of organizations migrate data to Cloud Storage providers.

### 4.1 Related work

In healthcare domain, the cloud-computing paradigm is expected to provide an environment perfectly matching the needs of collaborating healthcare workers (Fabian et al., 2015), (Ermakova et al., 2013) Security and Privacy System Requirements for Adopting Cloud Computing in Healthcare Data Sharing Scenarios, (Kanagaraj et Sumathi, 2011) Proposal of an

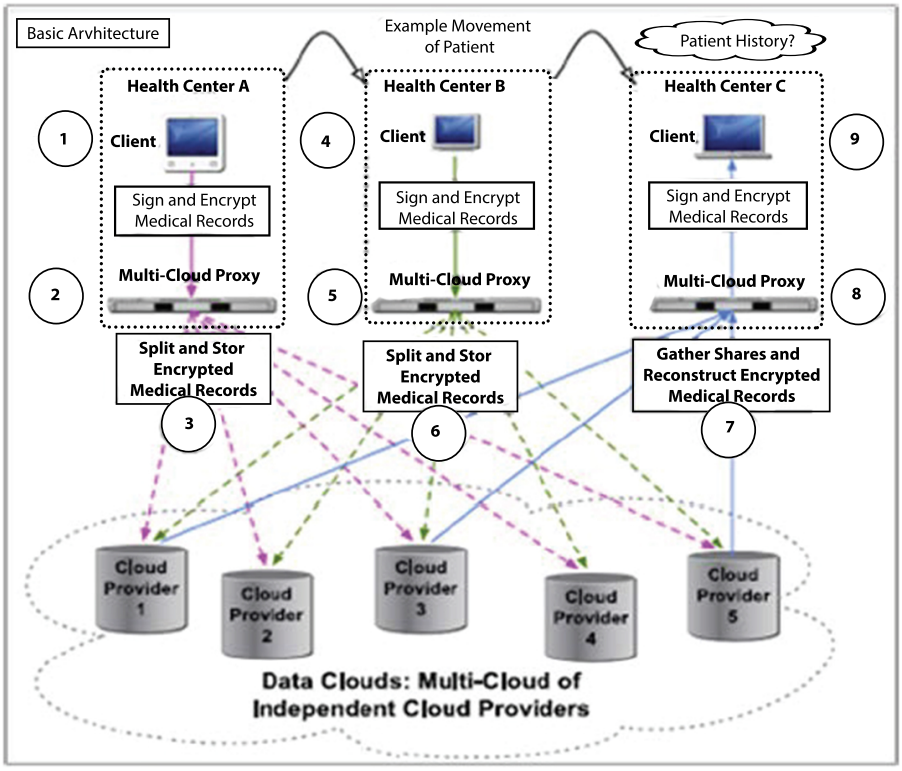


FIG. 1 – *Architecture overview.[1]*

Open-Source Cloud Computing System for Exchanging Medical Images of a Hospital Information System.

## 4.2 Description of problematic

In (Fabian et al., 2015), authors realized a solution of a novel architecture (figure 1) and its implementation for inter-organizational data sharing, which provides a high level of security and privacy for patient data in semi-trusted cloud computing environments.

The principle of this architecture is to share the medical record (MR) of each patient in the different health center with a high level of security and privacy for patient data in semi-trusted cloud computing environments, by using MCP by the side of Client.

Proxy Multi-Cloud acts as an intermediary between clients and stored data in different Cloud providers. Its objective is to provide authenticated and authorized customers with a secure storage center, which also involves secret sharing techniques.

## 4.3 Problematic challenges

This architecture has a lot of benefits on the side of confidentiality of user access privileges, and also security and privacy measures (Fabian et al., 2015). One of the biggest challenges here is the recovery of stored data. For one request, MCP must search the data requested into all different Cloud providers, which can brings some drawbacks such as :

### 4.3.1 Network challenges

SaaS applications in the cloud and made accessible via a network to the SaaS consumers (Hogan et al., 2011) In the case of the architechture, we can extract some drawback such as :

- **Security :** The cloud is utilized by organizations in several service models (saas, paas, and Iaas) and in deployment models (public, private, hybrid, and community). There exist a number of security worries connected with cloud computing. Yet, these matters are classified into broad sets security issues confronted by cloud providers. In this case Security is also critical because of the large coupling between MCP and Cloud providers ; decrease the level of security of data into Clouds ;
- **Coupling :** For the recovery of patient data from Clouds, the MCP must send the request to all of different Cloud providers, which increases the coupling between MCP and Clouds ;
- **Network overload :** When a proxy receives a request from customers, this request will be multiplied by the number of Cloud providers, which increase the traffic on the network. For example, if we have two requests, one from healthcare center A and another from healthcare center B, between proxy and Cloud providers, we will have five requests for each proxy so the number of request will be ten. So for two demands, we will have ten requests from the proxy ;

### 4.3.2 Interoperability challenges

Interoperability may be assessed in terms of the NIST Cloud Computing Reference Architecture at the IaaS, PaaS, and SaaS levels. Each of these levels, which may be combined in any particular Cloud service or product in practice, presents special considerations, and as a result, the standards landscape is intrinsically unique and specific to each level. In the case of the architechture, e can extract some drawback such as :

- **Environment heterogeneity :** Enterprises think that it is simple to add one Cloud service at a time and they do not expect the inevitable complexity of multiple Cloud providers for integrating their applications running on different Cloud platforms which end up with a traditional way of point-to-point integration approach. So, enterprises need to think about the complexity on integration of multiple applications on different Cloud platforms along with on premise applications and also think about service access technology used by (Kolluru et Mantha, 2013) ;
- **Standardization :** Is one of the most problems in the Cloud environment, many of their interfaces offered are unique to a particular provider, also the risk of provider lock-in is raising (Kress et al., 2013). Simon Wardley said in (Wardley, 2008), (The ability to switch between providers overcomes the largest concerns of using such service provi-

ders, the lack of second sourcing and the fear of vendor lock-in (and the subsequent weaknesses in strategic control and lack of pricing competition)) ;
– **Complexity of multiple Clouds :** The use of multiple Cloud providers in big systems increases the level of communication complexity between Cloud providers, also choosing the technology service access compatible with technology used increase the level of complexity.

# 5 Proposed Solution

## 5.1 Discription of our solution

Our proposal solution (Figure2) consists on adding a new Private Central Proxy Cloud (2PC) to improve architecture proposed (Fabian et al., 2015) and presented in figure1. This new Private Central Proxy Cloud is inserted between health centers MCP and Cloud providers. The main objective of the new Private Central Proxy Cloud added is to minimize coupling between MCP and Cloud providers, and also to increase the level of security of data and minimize network overload. 2PC will be the intermediary between MCP and Cloud providers. Thus, for each request, the MCP searches the specific Cloud provider which contains the desired data, by using a table which connects each external identifier with the Cloud provider which contains stored data. In this case, 2PC helps to store data in specific Cloud providers and memorizing the location of each data. 2PC stores all information about location of every Patient data in Cloud provider. All that helps to recover data stored easily from Cloud providers without searching in all Cloud providers.

The MCP both acts as a web-service server and client. In this architecture, we propose SOAP web service interface to communicate between Cloud and proxy, to allow authenticated clients storing Data as encrypted shares in the clouds. 2PC also acts like MCP focusing on data location of each patient. Private Central Proxy Cloud features adding to the benefits of SOA in the new schema show the main features and benefits of the whole process.

## 5.2 Main features of our proposed Cloud

The figure below presents our proposed solution. It is based on a Private Central Proxy Cloud. Our proposed Cloud is private because it should be accessible only in existent Healthcare system since manipulated data are sensible and must be consulted only by Healthcare system users. Access to our 2PC from public must be denied. Our proposed Cloud is not attached to existent date Clouds, it ensures communication between those existent data Clouds and Healthcare system users. Thus, the Healthcare system users access to existent date Clouds via our proposed Cloud. So among the main features of our Cloud is that it is central and proxy. Our proposed solution can be generalized to any system in which users must access to private data stored in multiple private Clouds like data students system in Educational Institutions. The added Cloud must also be private, central and proxy to ensure data security and communication between system users and existent multiple data Clouds.

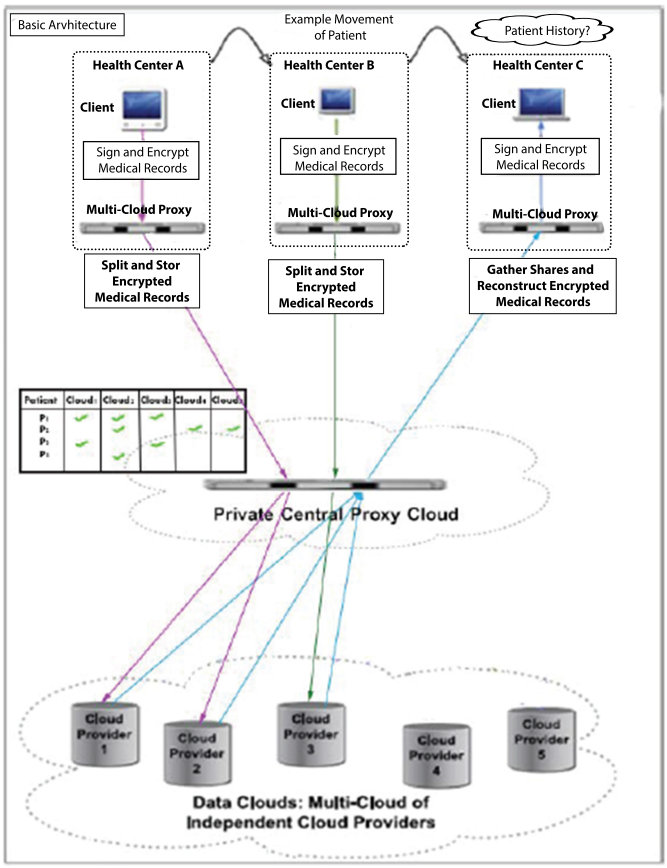


FIG. 2 – *Sample process of proposed solution*

## 5.3 Benefits of this solution

Proposed solution shows the main features and benefits of the whole process.Benefits are divided into two levels ; the network level and interoperability level, Some of these benefits are :

### 5.3.1 Network benefits

Network is important in communication enter Consumer and Cloud provider, for that our proposition brings some benefits in network such as :

– **Tight coupling :** Objective was to eliminate multiple communications between MCP and Cloud providers such as distributed architectures typically link components directly to one another, by centralizing all information about data storing of each Patient ;

- **Easy MR recovery :** Our idea is to centralized information about location of each MR patient in different Cloud providers, all of that to facilitate data recuperation ;
- **Network overload :** When a proxy receives a request from customers, this request will be multiplied by the number of Cloud providers. In our proposed architecture, 2PC defines specific Cloud provider which contain data of specific patient which decrease the traffic on the network ;
- **Security :** Hand in hand with SOA and multi-level authentication in both MCP and 2PC and Web Service Security protocols, the access of data will be more secure. Also minimizing multiple communications between MCP and Cloud providers increases the level of security.

### 5.3.2 Interoperability benefits

The big problem for client in Cloud provider is standardization because Cloud Computing is not mature as SOA, and many of the interfaces offered are unique to a particular vendor, thus raising the risk of vendor lock-in. For that, the 2PC can be able to communicate with the most of interfaces using technologies of SOA ;

- **Management of access users :** Management of users also is controlling by the 2PC and every access to the data by access control ;
- **Using multiple Cloud :** In case of using multiple cloud environment, Cloud consumers can use and controle multiple cloud easly ;
- **Easy Maintenance :** Is one of advantages of centralization is maintainability.

## 6 Conclusion and perspectives

Currently, the public SaaS is the service model of the most popular Cloud that consists of making available ready applications to the world. At this level, the offer is very rich : it is now possible to find solutions for SaaS almost all traditional needs (email boxes, CRM, storage, video editing ...). There are real opportunities there are not to be missed.

In this paper, we have presented a thoughtful description of SOA and different types of Cloud Computing. Case study solution between Cloud providers and MCP has been suggested in order to facilitate data recuperation from Cloud provide, and decrease network overload between MCP and different Cloud, and also to immunize the problem of standardization. Hence, we introduced a notion of adding a Private Central Proxy Cloud between health Center MCP and Cloud providers. Our solution gives very important benefits such as tight coupling between MCP and Clouds facilitate data recovery, increasing the level of data security, minimizing the level of problem of Standardization, management of access user by the costumer and controlling communication between Cloud providers by the 2PC. In perspective, we aim for supporting more interfaces between Cloud providers and 2PC.

## Références

Cartright, I. et E. Doemenburg (2006). Time to jump on the bandwagon in it. *British Computer Society, UK*.

Ermakova, T., B. Fabian, et R. Zarnekow (2013). Security and privacy system requirements for adopting cloud computing in healthcare data sharing scenarios.

Fabian, B., T. Ermakova, et P. Junghanns (2015). Collaborative and secure sharing of healthcare data in multi-clouds. *Information Systems 48*, 132–150.

Goyal, V. et A. Jain (2012). Role of soa & cloud computing in it industry. *International Journal of Engineering 1*(6).

Hogan, M., F. Liu, A. Sokol, et J. Tong (2011). Nist cloud computing standards roadmap. *NIST Special Publication 35*.

Kanagaraj, G. et A. Sumathi (2011). Proposal of an open-source cloud computing system for exchanging medical images of a hospital information system. In *Trendz in Information Sciences and Computing (TISC), 2011 3rd International Conference on*, pp. 144–149. IEEE.

Kaur, P. D. et I. Chana (2014). Cloud based intelligent system for delivering health care as a service. *Computer methods and programs in biomedicine 113*(1), 346–359.

Kolluru, N. V. S. et N. Mantha (2013). Cloud integration, strategy to connect applications to cloud. In *India Conference (INDICON), 2013 Annual IEEE*, pp. 1–6. IEEE.

Kress, J., H. Normann, D. Schmiedel, G. Schmutz, B. Trops, C. Utschig-Utschig, et T. Winterberg (2013). Industrial soa soa blueprint : A toolbox for architects.

Mahmood, Z. (2007). The promise and limitations of service oriented architecture. *International journal of Computers 1*(3), 74–78.

Wardley, S. (2008). Cloud recap... the cloud today.

## Summary

In Collaborative and secure sharing of healthcare data in multi-clouds, Fabian, Ermakova and, Junghanns realized a solution of a novel architecture that externalizes data and its implementation for inter-organizational data sharing, which provides a high level of security and privacy for patient data in semi-trusted cloud computing environments, using Multi-Cloud Proxy by the side of Client.the focus of our article is to propose a solution by using a Private Central Proxy Cloud implemented in a private Cloud environment, which can be an intermediate between different Cloud providers and health centers. All that to get benefits such as tight coupling, increasing the level of security, minimizing network overload problem and recovering data easily.