International Journal of Clinical & Medical Informatics

**ISSN: 2582-2268** **Research Article** | Vol 1 Iss 2

# Designing Secure Cloud-Based Solutions for Several Teleconsultation Scenarios

**Isabel de la Torre-Díez[1], Sofiane Hamrioui[2], Beatriz Sainz-de-Abajo[1*], Eduardo Motta Cruz[2] and Miguel López-Coronado[1]**

[1]Department of Signal Theory and Communications, and Telematics Engineering University of Valladolid, Paseo de Belén, Valladolid, Spain

[2]Bretagne Loire and Nantes Universities, IETR Polytech Nantes, France

[*]**Corresponding author:** Beatriz Sainz-de-Abajo, Department of Signal Theory and Communications, and Telematics Engineering. University of Valladolid, Paseo de Belén, 15, 47011 - Valladolid, Spain, Tel: +34 983423000 Ext. 3702; Fax: +34 983423667; Email: beasai@tel.uva.es

## Abstract

**Background: Cloud data centralization is a way to ensure patient safety and medical management. For a secure cloud-based teleconsultation, it is necessary to ensure optimum levels of security, as patients' data will not be in the same place from where it was accessed.**

**Objective: The aim of this work is to present two secure cloud-based solutions for a teleconsultation service in the following scenarios: an urban and rural health centre. The iCanCloud software was used to simulate teleconsultation in these different scenarios.**

**Methods: The urban health centre was a city in Spain that, attends around 107,000 adult and 16,700 paediatric consultations per/year. In the second scenario, the health centres in rural Spain attended an average of 437.08 patients a month and around 15.7 a day.**

**Results: After methodology analysis and scenarios description, the proposed solutions for each of them are shown and justified by a theoretical explanation that could prove useful when establishing real future situations.**
**Conclusions: Thanks to the research conducted on cloud computing technology, it was possible to provide a personalized solution in the form of a teleconsultation service for city and rural health centres in a private and secure way.**

**Keywords:** ***Cloud; Secure solutions; Health centre; iCanCloud; Scenarios; Teleconsultation***

**Received Date:** October 24, 2018; **Accepted Date:** October 31, 2018; **Published Date:** November 07, 2018

## Introduction

The combination of cloud computing with e-health services can provide a virtual view of resources irrespective of the

**Citation:** Torre-Díez IDl, Hamrioui S, Sainz-de-Abajo B, et al. Designing Secure Cloud-Based Solutions for Several Teleconsultation Scenarios. Int J Clin Med Info 2018: 1(2) 65-72.

geographic location or physical space [1-3]. Given that the data will not physically be in the same place as to where it was accessed, special care needs to be taken when requesting such services. Security and privacy are essential factors to take into consideration [4,5].

One of the essential problems to address is stored, as a large amount of patients' health records will be stored in the cloud. Additionally, images (for example in DICOM format) will also be stored in certain cases [6-9]. The storage systems on the cloud are among the most successful applications nowadays. One needs to take it into account the storage systems on the cloud, the different types, systems and security copy software and use of shared files, as well as to ensure that cloud-based storage systems can be interactive [9-11].

Any cloud-based storage solution must comply with authentication when starting a session, high encoding (at least 128 bits) of data transfer from end to end, and data compression without loss [11-13]. Previously, Fernández-Cardeñosa et al. [14] proposed two examples of cloud-based solutions for Electronic Health Records (EHRs). Rodrigues et al. [15] analyzed the security requirements of EHR solutions on the cloud. These authors proposed different secure and robust cloud-based solutions for equipping a set of rural health centres near Valladolid, Spain with e-health services such as EHRs, telecardiology and telediagnosis [16]. Torre-Díez et al. [17] presented a secure, cloud-based solution for a telecardiology service in several scenarios.

The objective of this article is to present secure cloud-based solutions for a teleconsultation service in different scenarios: a city and rural health centres in Spain. The theoretical solutions may prove useful for establishing real future situations.

The points that will be covered in this paper are a description of the scenarios proposed and, a secure solution for each scenario.

## Methods

The scenarios will be analyzed separately in this section, depending on the type of location, we will take into account the type of storage used, according to each e-health application, the infrastructure used security and privacy policies, the volume of patients the staff at each centre and skills levels. As in [16,17], the iCanCloud software was used to carry out the simulations within the different scenarios that, provided a modelled physical structure in which users were able to work [17].

Data from each centre was estimated in comparison to real cases to show solutions that are as realistic as possible. Therefore, the scenarios in which a theoretical cloud computing solution was considered for a teleconsultation application was a health centre in the city and rural areas.

### First case study: City health centre

A health centre in Spain is about 2,500 square metres and provides services to 40,000 inhabitants; however, these numbers are not comparable to a city hospital. The example of this study was "the Ciudad Jardín" Health Centre (Córdoba, Spain), which has 26 offices for doctors and nurses, 8 for paediatric consultations, one multi-purpose room and, several other rooms for extractions and treatments, dentistry, minor surgery and health education. The centre also has a large service and administrative areas [17]. The Government Delegate for Health, Baena [17] estimated that centre attends around 107,000 adult and 16,700 paediatric consultations. These data were used for estimate the number of electronic health records.

The use of EHRs in this scenario is imperative, as a large volume of information is used on a daily basis and frequently in this type of health centre. In this context, electronic health records imply treating text, with some descriptive image. Neither a large flow of information nor high-quality images are required. In this scenario, the cloud computing solution should not attempt to be a large-scale storage system, as occurs in the case of a city hospital [17].

The cloud computing solution for the city health centre offered optimum performance that focuses on teleconsultation applications. The information that doctor requires was saved, and later retrieved if needed at the centre or via data transmission.

Only doctors who provide treatment of referrals were authorized to modify or carry out any operation regarding patients' clinical data.

### Second case study: Rural health centre

These are health centres that offer basic care in rural areas, serious cases or those requiring specialist care were referred to the nearest hospital. In rural health centres in the province of Valladolid, 5,677 patients were attended at an average of 437.08 patients a month and around 15.7 a day [17]. Most cases, around 93% were treated at the health centre itself, whereas 6.8% were referred to the nearest hospital. The example studied was located in an area of around 8,560 inhabitants and provided coverage to small nearby villages as well, thus the flow of patients was variable and could not be estimated accurately [17].

### Results

The research was expanded into a range of encoding technologies, digital signatures, tools and technologies to be able to provide an effective, viable solution for proper authentication by health professionals. A decision was made to implement the use of smart cards in the system for maintaining a person's identity in the cloud computing system, and cloud-based e-health application in any situation.

As it was explained in De la Torre et al. [16], the computer or computers located in the rooms are equipped with a CAD (Card Acceptance Device), which is a smart card reading device where the client part system takes charge [17]. This is sufficient for a JVM (Java Virtual Machine) and an OCF (Open Card Framework) bookstore. A smartcard's Open Card Framework or OCF is merely a type of middleware implemented in Java that enables an application to be aware of the presence of the card and be able to interact with it in accordance with the ISO/IEC 7816-4, -8 and -9 standards [17]. All this interacts jointly with the system's healthcare software in each terminal, where the CAD is located. The OCF is located between the CAD and the host application that is in the PC. It is expected that the OCF can integrate with the smartcards destined for healthcare systems [16,17]. There is also an object known as the Card Manager which will was responsible for starting and shutting down the computer and establishing a secure communication channel between the smart card and the open session at any specific time. This data was handled by the objects known as Doctor Session and Patient Session, and the communication was assured via the APDU (Application Protocol Data Unit). Furthermore, the smart card terminals act as clients in the RMI protocol by calling remote objects. The client equipment did not contain any software that takes charge of accessing the data-bases and making consultations. Instead, the remote objects took charge of this, the client software contained only the user's interface components (instances of Java classes) and ways of displaying the MVC (Model View Controller) layers of architecture.

Figure 1 shows the RMI server part, which in this case was the load balancer that is an application Server when the former was implemented on the cloud. Secure authentication of the data stored on the cloud was obtained and its privacy assured. When a

client wishes to update information about a patient on the clinical data-base, they call the remote object data in an encrypted and signed format. Then the data is sent to the RMI server thread via the RMI channel on TCP/IP with parameter marshalling. The thread then prepares the data and sends it to the remote object. Therefore, the remote object controls the client's authentication, decode the data, prepare a suitable consultation and update the data on the remote data-base. The result of the operation is returned to the client using the same channel.

Thus, all the control and connection operations of the data-base are provided to the clients-in this case to the relevant doctors. The remote controls in RMI servers comply with such operations on clients' behalf and the MVC (Model View Controller) layer of the system's architecture.

Thanks to the Java technology being implemented (see JDBC in Figure 1) and the smart card we are able to obtain authenticated secure access to the cloud data base using a secure channel on TCP/IP. This protocol is present in all communication and should not cause any problem when connecting from one point to another.

**Teleconsultation service at a city health centre**

Secure authentication is assured via smart cards, using Storage GRID technology.

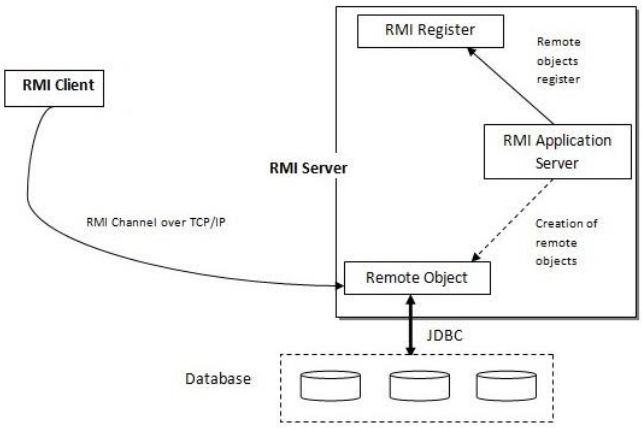


**Figure 1:** RMI server part.

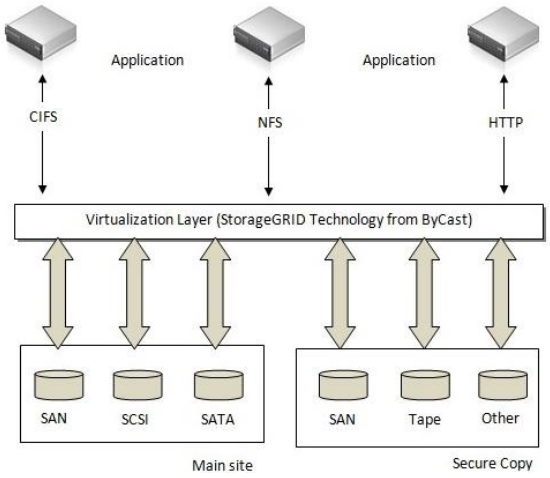


**Figure 2:** Cloud storage system with tolerance to errors. By Cast StorageGRID.

Figure 2 below shows how the StorageGRID works. StorageGRID is a virtualization software that can be used on the data-base server to create a type of virtualization that combines storage of different devices in a single administrative system. In terms of output, data storage petrabytes can be combined, different types of storage systems used, and protocols transported over geographically scattered locations. The StorageGRID is able to administer data from NFS (Network File System) and CIFS (Common Internet File System) file systems on HTTP (Hypertext Transfer Protocol) networks. This is very useful as we can interact with NFS and CIFS with SAN (Storage Area Network) file Systems that will be an NTFS (New Technology File System) to enable the data base to be treated as BLOB objects. The data can be replicated, migrated to different locations and also recovered in the event of shutdowns. The degree of replication can be configured, and when storage fails, StorageGRID can be recovered with other copies of data contained in the systems. These features make it one of the most important tools within the cloud.

Figure 3 shows a theoretical solution to the teleconsultation service that is fully implemented in the cloud. With this solution, the doctor in the city health centre can be authenticated in the cloud-based system using their smartcard; they will gain secure access to the data-base on the patient who is being treated at that time.

Given that there is no teleconsultation service at the health centres, it is necessary to have a scenario where the cardiologist can communicate with the doctor at the city health centres. The doctor has access to the data on the cloud on which they are interacting with the doctors at the health centres. With this solution, the doctor can communicate securely. Thanks to this infrastructure, the system enables a city health centre without teleconsultation service to communicate with the nearest hospital, so as to offer the services that a smaller centre lacks.

### Teleconsultation service at rural health centres

As shown in the previous cases, there are common features in the secure authentication via smart cards and the use of StorageGRID technology. The data base and web servers perform the same tasks together with the agent, and the load balancers will remain essential for this solution.

There must be communication with the hospital in order to obtain teleconsultation support. A cloud-based cardiology connection infrastructure is required at the nearest hospital to provide teleconsultation support at the rural health centres.

In Figure 4 we can see the implementation of cloud computing technology for a teleconsultation e-health application in a rural health centre environment. We used load balancers and various web servers to support all the requests entering the cloud-based system. The number of requests could be high due to the uneven population distribution existing in the different municipalities. The local images can be created using the cardiologist's electronic tools at the hospital, and uploaded onto the cloud. Once the applications server has finished processing the image, recorded the data-base, and returned the result to the web server the physician can display the result and take any decisions as they see fit. In terms of security, the information channels via firewalls and the use of the proxy/web-agent with the respective encoding keys, and the BLOB + SAN (RAID 0+1) file systems with back-up copy and administered using StorageGRID.

The only infrastructure required is to upload data onto the Internet.

A type of private cloud is proposed in all scenarios, and the estimated cost was similar in all cases if we assume that the same

Internet speed will be available (theoretically around 1 Gbps), with cost around €450/month [16,17]. Table 1 shows the most significant features of the solutions proposed for the two scenarios analyzed.

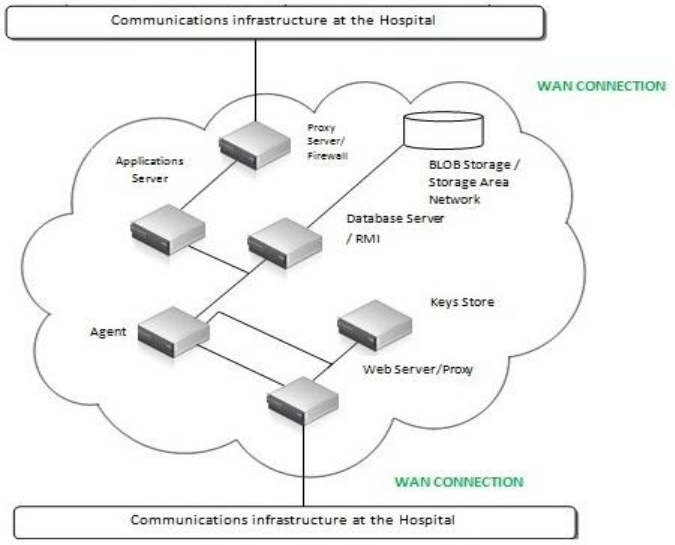


**Figure 3:** Diagram of the cloud-based infrastructure for full implementation of teleconsultation at a city health centre full implementation.

## Discussion and Conclusion

Many health centres are becoming overwhelmed by the growing amount of information they need to process and administer. Using systems like the one we described, doctors can devote more time to patients by automating the recording, administration, and consultation of health records information. The use of cloud computing technology together with e-health applications constitutes a major step in both the quality of treatment provided to patients and the work accomplished by healthcare staff.

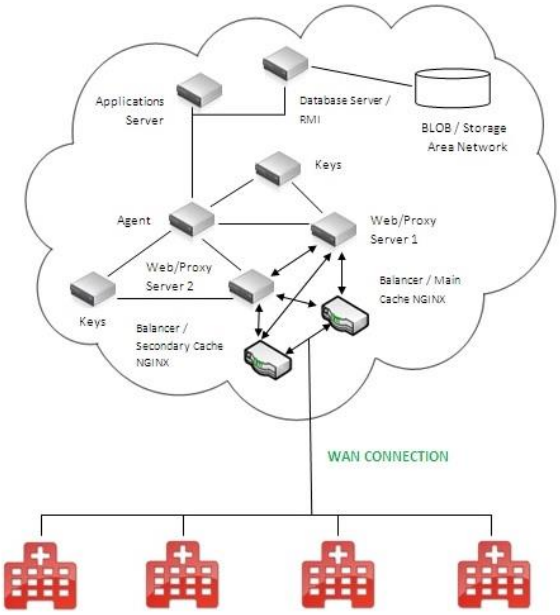


**Figure 4:** Diagram of the cloud-based infrastructure for full implementation of teleconsultation at rural health centres.

Cloud computing technology was detailed in this work to explore whether secure solutions for cloud-based teleconsultation can be provided via the cloud, what infrastructure would be viable for this proposal and whether it could be implemented while ensuring the protection of patients' data. It was possible to centralise information on the cloud by offering facilities that improve the use of the system in a fast and simple way, resulting in better treatment for the patient.

| **Type of scenario** | **Elements required to ensure security** | **Suitable connection speed** | **Type of cloud** | **Monthly price of the solution (€/month)** |
|---|---|---|---|---|
| A health centre in urban areas | Smartcards<br>StorageGRID technology<br>Load Balancer<br>2 Web/Proxy servers | From 1 Gbps | Private | 450 |
| A health centre in rural areas | Smartcards<br>StorageGRID technology<br>2 load balancers<br>2 Web/Proxy servers | From 1 Gbps | Private | 450 |

**Table 1:** Summary of solutions for both scenarios.

Controlling access to the system, the use of firewalls configured with IP Failover, the greatly-enhanced security offered by the use of encoding keys via the Proxy and the agent and storage system being proposed, enabling secure copies to be created within the cloud, increasing the security of all communication, and also ensure the robustness of the data. Thanks to the research on cloud computing technology, together with other technologies required to provide the system with excellent authentication, an adapted solution has been created for a teleconsultation service in a city and rural health centers, offering security, privacy and robustness for a large number of cloud-based requests.

The use of cloud-based computing technology alongside the smartcard system was proposed for doctor's authentication helps healthcare centres to electronically administer all patients' health data, enabling the former to reliably update and modify. such information. Any authorized physician or health professional may access the services provided by several e-health applications at any time and from any location in the different scenarios.

## Acknowledgements

This research has been made within the Program "Movilidad Investigadores UVA-BANCO SANTANDER 2018", and it has been partially supported by the European Commission and the Ministry of Industry, Energy and Tourism under the project named "A persuasive system supporting Memory and Moments of people with the Early and Middle stage of dementia".

## References

1. Cloud Computing, CSA (Cloud Security Alliance) (2018).
2. Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration, Jericho Forum. Version 1.0, April 2009.
3. Sarathy V, Narayan P, Mikkilineni R, et al. (2010) Next Generation Cloud Computing Architecture: Enabling Real-Time Dynamism for Shared Distributed Physical Infrastructure. In: 2010 19th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE'10), Larissa, Greece 48-53.

4. Rochwerger B, Breitgand D, Levy E, et al. (2009) The Reservoir model and architecture for open federated cloud computing. IBM Journal of Research and Development 53(4): 1-11.
5. SUN Microsystems (2009) Introduction to cloud computing architecture, White Paper, 1st (Edn).
6. Marcheschi P, Mazzarisi A, Dalmiani S, et al. (2004) HL7 clinical document architecture to share cardiological images and structured data in next-generation infrastructure. Computers in Cardiology 617-620.
7. Smith D, Newell LM (2002) A physician's perspective: deploying the EMR. Journal of Healthcare Information Management 16(2): 71-79.
8. Lo HG, Newmark LP, Yoon C, et al. (2007) Electronic health records in specialty care: a time-motion study. Journal of the American Medical Informatics Association 14(5): 609-615.
9. Margan A, Rustemović N and Loncarić S (2005) Virtual polyclinic--consultant health service for rural areas and islands. Acta medica Croatica: casopis Hravatske akademije medicinskih znanosti 59(3): 169-178.
10. Tunali T, Yildirim S, Dalbasti T (2002) The use of smart cards in health care. Hermes Project Workshop 1-6.
11. Hansmann U, Nicklous MS, Schäck T, et al. (2012) Smart card application development using Java. Springer Science & Business Media.
12. Church P, Goscinski A and Lefèvre C (2015) Exposing HPC and sequential applications as services through the development and deployment of a SaaS cloud. Future Generation Computer Systems 43: 24-37.
13. Anselmi J, Ardagna D and Passacantando M (2014) Generalized nash equilibria for saas/paas clouds. European Journal of Operational Research 236(1): 326-339.
14. Fernández-Cardeñosa G, de la Torre-Díez I, López-Coronado M, et al. (2012) Analysis of cloud-based solutions on EHRs systems in different scenarios. Journal of Medical Systems 36(6): 3777-3782.
15. Rodrigues JJ, De La Torre I, Fernández G, et al. (2013) Analysis of the security and privacy requirements of cloud-based electronic health records systems. Journal of Medical Internet Research 15(8): e186.
16. de la Torre-Díez I, Lopez-Coronado M, Soto BGZ, et al. (2015) Secure cloud-based solutions for different eHealth services in spanish rural health centers. Journal of Medical Internet Research, 17(7): e157.
17. de la Torre-Díez I, Garcia-Zapirain B, López-Coronado M, et al. (2017) Proposing telecardiology services on cloud for different medical institutions: a model of reference. Telemedicine and e-Health 23(8): 654-661.