Journal of Theoretical and Applied Information Technology
15th April 2019. Vol.97. No 7

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SECURE CLOUD-BASED PICTURE ARCHIVING AND COMMUNICATION SYSTEM FOR DEVELOPING COUNTRIES

[1]ADEBAYO OMOTOSHO, [2]JINMISAYO ADIGUN AWOKOLA, [3]JUSTICE ONO EMUOYIBOFARHE, [4]CHRISTOPH MEINEL

[1]Lecturer 1, Landmark University, Department of Computer Science, Omu-Aran, Nigeria

[2]Resarch Scholar, Ladoke Akintola University of Technology, Department of Computer Science and Engineering, Ogbomoso, Nigeria

[1]Professor, Ladoke Akintola University of Technology, Department of Computer Science and Engineering, Ogbomoso, Nigeria

[1]Professor, University of Potsdam, Hasso Plattner Institute (HPI) for IT Systems Engineering, Potsdam, Germany

E-mail: [1]omotosho.adebayo@lmu.edu.ng, [2]rhgonline@gmail.com, [3]eojustice@gmail.com, [4]meinel@hpi.de

ABSTRACT

Picture Archiving and Communication Systems (PACS) are used to enable medical images from imaging modalities to be stored electronically and viewed on screens so that medical practitioners and other health professionals can access them. However, PACS comes with a lot of costs for storage, air conditioning licenses and so on, these necessitate the need to take advantage of existing technologies that can enhance adoption, especially in developing countries. More alarming is that data centres for electronic health services have been the target of several attacks and hacks in recent year, even though cloud computing has the potential of making the adoption of PACS more cost-effective. Cloud computing has a major drawback in the area of security. In this work, a framework for securing cloud-based PACS is developed and implemented.

Keywords: *E-Health, Telemedicine, PACS, Cloud Computing, Security, Modalities, Medical Images, Privacy*

1. INTRODUCTION AND BACKGROUND

Images play a very vital role in health care as the diagnosis and treatment of some types of diseases borders around capturing, processing and interpreting images of some body parts. Picture Archiving and Communications System (PACS) enables medical images, from imaging modalities such as x-rays and scans, to be stored electronically and viewed on screens, so that medical practitioners and other health professionals can use the information for further analysis and diagnosis [1]. In the past, a film has been almost the only medium for capturing, storing, and displaying radiological images. The film is a fixed medium with usually only one set of images available, while PACS has facilities for multiple views [2]. PACS could be quite expensive to maintain and this is the major reason many hospitals in developing countries stick to the traditional way of archiving radiological images [3, 4]. The costs connected with PACS - apart from the cost of acquiring and installing medical imaging instruments – include: software costs (development, security, maintenance and license costs), hardware costs (various computers and workstations to interface with the equipment), storage costs (acquiring servers that would archive the images), electrical power costs (for keeping image servers and other equipment on consistently), air-conditioning and other related costs [5]. It is therefore imperative to take advantage of technologies that can help in delivering the effectiveness of PACS at a minimized cost. One of such recent technologies that have the potential of making the adoption of PACS more cost-effective in terms of storage is cloud computing [6].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Cloud computing involves the provision of on-demand scalable resources such as networks, servers and applications [7, 8, 9]. These resources are provided as a service and are accessible to end users. They can be readily provisioned and released with minimal effort or service provider interaction. Cloud computing has five major defining characteristics namely; on-demand self-service, ubiquitous network access, location transparent resource pooling, rapid elasticity and measured service with pay per use. Cloud computing has significantly helped individuals and organizations to reduce capital investments in hardware and software [10,11,12]. It has also helped in reducing the complexity of owning and operating computer resources. Cloud services can be deployed in form of Private, Public or Hybrid Clouds. Layers of Cloud computing services comprises; Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Service. However, adopting cloud computing comes with some challenges [13]. The major challenge associated with cloud computing is security [14, 15, 16]. Data migrated from the user's end is moved to a cloud service provider's server but, there is no guarantee that the service provider would not infringe on the client's data by either accessing it or copying it without the client's permission or authorization [5]. Hence, there is a high probability that data breach might occur on the other side. Since so many clients move their data to cloud platforms, it may be difficult for individual data owners to claim complete ownership of their data on the cloud. Hence, security-related issues must be a major consideration before deploying cloud-based solutions. Also, migrating sensitive data to the cloud would require clients to enforce data privacy and ownership [17]. In cloud computing, financial and medical data of every kind are referred to as sensitive data [7]. This work addresses this issue by developing a security framework for cloud-based PACS.

[18] worked on a cloud security model and in their findings, e-health clouds impose a variety of security and privacy risks. The work proposed to wrap a secure e-health infrastructure on Trusted Virtual Domains (TVDs) to ensure fundamental security and privacy properties. However, the solution provided in their work is limited in that it considered only the end users side in its security. [19] worked on cloud-based Automated Medical Image Collection Annotation (AMICA) toolkit in which a range of content analysis functions was provided to tag images and images regions. The user uploads a Digital Image and Communication in Medicine (DICOM) file to an online portal and the software finds and displays images that have similar characteristics. AMICA was developed to run in the Microsoft cloud environment using the Windows Azure platform to cater for the storage requirements of typical large medical image databases. This work, however, did not provide a major security function, thus leaving the DICOM Images at the risk of unauthorized access and other forms of security breach. [20] designed a system that provides appropriate management of oncology patient records, and provides privacy to patient textual and DICOM image information by anonymizing them. Personal Data (PDATA) and Clinical Data (CDATA) were identified from the DICOM images retrieved from the PACS server. The role-based policies were implemented and stored in the database which was used for the anonymization of PDATA. The anonymity algorithm was successfully implemented and deployed on Google App Engine. This work, however, is limited in application as it only takes care of oncology DICOM Images alone, which are usually of a single imaging modality in most cases. The anonymization algorithm used in this work also did not state clearly the way in which Pixel and Metadata were split in the DICOM Images. [21] explored the application of cloud computing to share medical imaging data across different institutions. Their architecture is shown in Figure 1 which describes a solution to share DICOM services across healthcare institutions without breaking DICOM based on the cloud. The main idea of this work is to promote DICOM inter-institutional communications, allowing the establishment of shared workflow and exchange of documents across them. The proposed DICOM relay service aims to be a communication broker, allowing the search, store and retrieve of medical images over a group of hospitals, in different sites. This solution allows, for instance, remote access to the institutional PACS archive. The issue of privacy and confidentiality of the medical images was not addressed in this work and this becomes a major challenge of moving the images to the cloud.

Our paper thus aims at developing a variant security framework for cloud-based PACS that combines existing security mechanisms in a way that addresses the security challenge of storing medical images on the cloud. The solution from this work is expected to enhance the security and adoption of PACS as a cloud service in developing countries

Journal of Theoretical and Applied Information Technology
15th April 2019. Vol.97. No 7

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

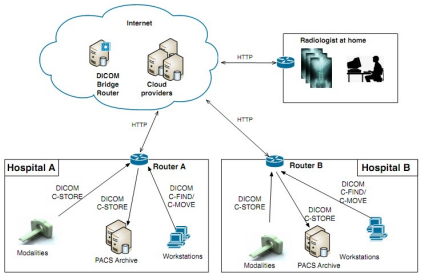

Figure 1: The Architecture of medical imaging across the cloud solution [5]

2. METHODOLOGY

2.1 The Proposed Cloud PACS Framework and Security Manager

The proposed framework is an improvement on existing work in the area of security that adopted the concepts of data obfuscation, authorization, and authentication. In order to further extend the scope of this framework, two cloud platforms were used to deploy and tests its performance. To provide a cloud PACS security solution, the different states of medical images throughout the stages of capturing, storage, retrieval are encompassed within the framework. Each state has a technique utilized in the security of data. Based on the analysis of the different states of data in the workflow, the following states and techniques were used in this framework:

(i). Data Residing on Client - Authentication, and Authorization: These are medical images residing on a workstation connected to the medical imaging device. The connection of this workstation to the Internet makes it capable to upload images to a cloud storage service provider. Access to images and other information is provided by the use of authentication and authorization techniques employed by the security manager.

(ii) Data in Transmission - SSL Encryption: The exchange of data across channels makes it vulnerable to hackers. This is also the case as PACS images are transmitted to the cloud via the Internet as a channel. To mitigate this vulnerability, an SSL encryption mechanism was employed.

(iii) Data in the Cloud - Obfuscation and Distributed Storage: As information is stored on cloud storage infrastructure provided by public Cloud Service Providers, these providers are the target to both internal and external security threats. In a bid to combat this threat, two techniques were combined; the use of data obfuscation and distributed information storage.

All these techniques were combined and implemented in the security manager which was integrated into the cloud PACS workflow. Figure 2 shows the detailed framework and Figure 3 illustrates the various security mechanisms that were adopted at different stages of the framework operation. The security model embedded in the PACS framework is called the Security Manager and it is shown in Figure 4. The security manager operates on a file sharing workstation at the client layer which is connected by a network agent. It executes different security mechanisms at different layers of the architecture and at different states. These are:

(i). Authentication and authorization at the client layer for accessing data at rest on the client.

(ii.) TLP/SSL encryption at the network layer for data in transmission through the network.

(iii.) Obfuscation and distributed storage of medical image files at the cloud layer for data at rest in the cloud

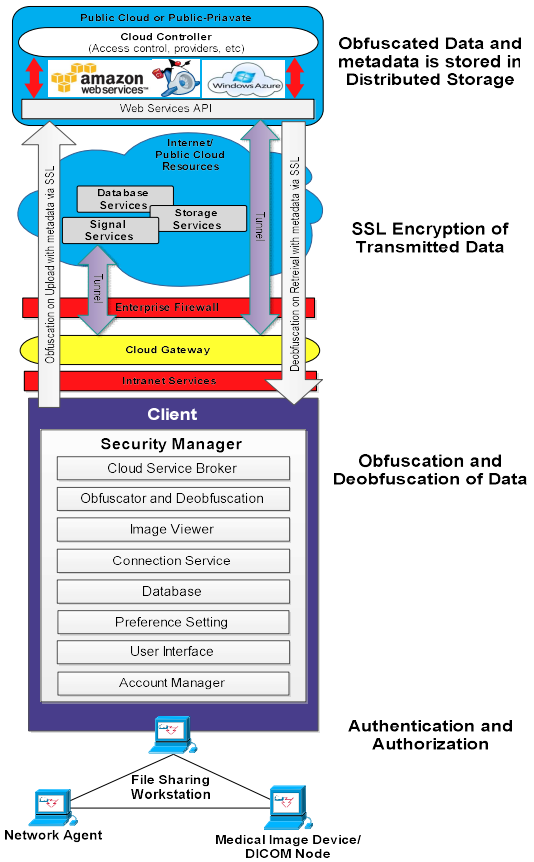

Figure 2: The complete cloud PACS Framework

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

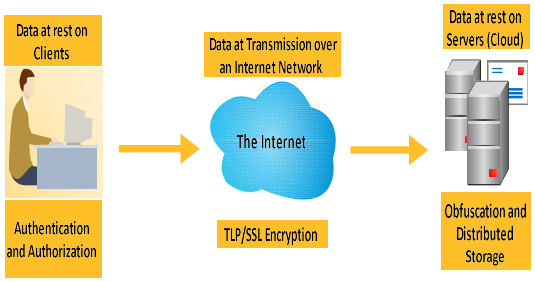

Figure 3: Security mechanisms at different states on the Secured cloud PACS

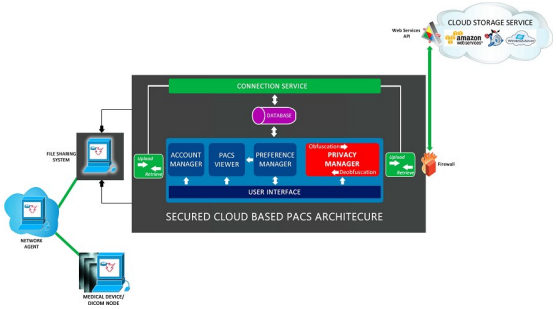

Figure 4: The Cloud PACS Framework Security Manager

2.1.1 Operational Components of the Secure Cloud-PACS Framework

The security manager inter-operate with other Cloud PACS standard modular protocols which are represented in the framework as the client, network, and cloud layers in order to successfully provide a secure cloud-based service for PACS users. The client layer comprises components such as medical imaging devices and workstations. The medical image devices are useful for capturing medical images by radiologists during the diagnosis process. The workstation aids in the medical diagnosis of images through the invocation of the Store-Forward-Query approach. The network layer consists of two major security components namely: enterprise firewall and cloud gateway. However, the enterprise firewall was used to block users outside the medical institutional domain of interest from accessing the cloud-plugged PACS-based repository. Also, the cloud gateway presents an interface between the local and remote (cloud) applications by ciphering the data. The cloud layer comprises of the following components namely: cloud resources, controller, and DICOM-to-Web-Services gateway. However, the major resource of interest in this layer is the storage infrastructure which was provided through Microsoft Azure and Amazon Simple Storage Service. The cloud controller component houses sensitive (confidential) information and is deployable through a trusted cloud service provider. Also, it provides security by logging different provider's unique credentials as well as controlled access to cloud resources. The DICOM-to-Web-Services gateway was used to bridge the barrier of implementing cloud-based PACS Server Implementation by ensuring interoperability between the DICOM devices and cloud interfaces. This is achieved by translating DICOM commands to web service requests since Internet Cloud Service providers only support web service API. The implementation was done using C# Programming Language.

The cloud PACS framework implemented a multi-objective security control to arrive at an optimal level of security by satisfying the data obfuscation, authentication, confidentiality (privacy), authorization and distributed storage security objectives through the security manager components. The components of the security manager are explained as follows:

(i.) User Interface - This component provides a graphical User interface for users to assess the different functionalities of the cloud-based framework. However, the users can query and visualize the query results securely via the user interface.

(ii) Account Manager - This security component enhances the multi-user and multi-tasking performance attributes of this framework. However, the data about the user's activities and its preferences are logged actively on the database connected to the account manager. Hence, users registered on the account manager can ubiquitously access the system securely.

(iii.)PACS Viewer - This provides a visualization interface for displaying medical images that are ready for subsequent content upload and download. This component automates the sorting of medical images based on informed preferences (image type and date).

(iv.)Preference Manager - This security component is intended for the proper management of the user's preferences. However, this is achieved by logging the preferences of the users in the database through a Graphical Preference Query Interface. Hence, the user's preference-driven database is securely connected to the internet so as to ensure the availability of logged preferential settings for specific users on the cloud-based PACS platforms.

(v.)Obfuscator and De-obfuscator - This security module implements the Yao's protocol to perform obfuscation and de-obfuscation. However, the encryption of image metadata (system catalog information) is the basis for satisfying the obfuscation security objective. This is achieved by encrypting the image metadata only that will be

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

stored in the cloud so as to enhance program-data independence in the security framework. Consequently, security and framework performance in terms of storage is achieved. De-obfuscator security module is responsible for de-obfuscating the obfuscated image metadata. De-obfuscation is achieved when the encrypted image catalog of information is reconverted into its initial information state.

(vi.) Cloud Service Broker - The cloud service broker component enhances the migration of PACS-based application to the cloud. The cloud service broker component uses the Secure Socket Layer mechanism to satisfy the confidentiality (privacy) security objective required at the network level of the framework. However, the cloud service broker abstracts the service distribution by mapping a user to a single service provider.

(vii.) Database - A Structured Query Language-complaint repository that is synchronized with the internet-based service provider was configured to ensure ubiquitous and secured access to the cloud-based PACS.

(viii.) Connection Service - This component enhances the operational functionality of this framework by providing a mechanism through which the required medical images could be successfully and securely uploaded, received, archived and transmitted in a cloud-based paradigm.

2.1.2 Operational Details of the PAC Framework

The selected Cloud Service Providers that were used at the deployment stage of this work were; Amazon Simple Storage Service (S3) and Microsoft Azure. The DICOM images used for the testing of the framework were acquired from three diagnostic centers in Nigeria. This is a step to localize the solution to the Africa/Nigeria context. The Internet connection present in the main campus of Ladoke Akintola University of Technology (LAUTECH), Ogbomoso was used to connect the framework to the cloud storage for storage and retrieval tests. The designed framework operates as follows:

(i.) The medical imaging device was connected to the file sharing system which also serves as host to the secured PACS application - the Security Manager (a novel application that was developed in this work which combines different security techniques for cloud PACS security).

(ii.) A user of the system registers and gets authenticated with his/her access credentials. Accessibility to files and operations was based on the authorization level of the user to the file. The connection stream communicates via web protocols (HTTP) to the Internet database for further authentication.

(iii.)The user of the system will access the images from the workstation for use, this can also be done using the developed DICOM viewer. The medical images to be uploaded to the cloud storage infrastructure were selected in the viewer.

(iv.)The medical image files or DICOM of different modalities selected for upload are distinctively separated into their component parts (that is Pixel data and metadata). A file map which is a directory of files was used to keep track of images and their corresponding metadata paired to them. It also contains a directory of Cloud Service Providers to which the security manager uploads the images to the cloud.

(v.)The metadata were obfuscated using the obfuscation function unique to each user with an account on the security manager. The security manager will connect to the Cloud Service Providers using a web service API of each of the Cloud Service Provider known by the file map.

(vi.)The anonymized Pixel data and obfuscated metadata were uploaded separately to the cloud storage service providers with the location of each tracked and updated into the file map. The images were uploaded through a TLP/SSL encrypted tunnel to prevent unauthorized access during the download.

(vii.)The users can select images for retrieval which are paired back to become a single entity by the file map. i.e. the images and their respective metadata retrieved from the cloud storage service providers.

(viii.)The images are downloaded through a TLP/SSL encrypted tunnel to prevent unauthorized access during the download.

(ix.)The obfuscated metadata of each image becomes de-obfuscated in the security manager after download using the de-obfuscation function unique to the user, and the medical image file or DICOM file becomes accessible to the user.

These operations can be performed by users from different locations as long as the security manager is available on their workstations. Users can upload medical image files from a location and access the uploaded images from another security manager on the workstation. The ubiquity of access - as seen in Figure 5 - is one of the core benefits of cloud PACS.

Journal of Theoretical and Applied Information Technology
15th April 2019. Vol.97. No 7

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

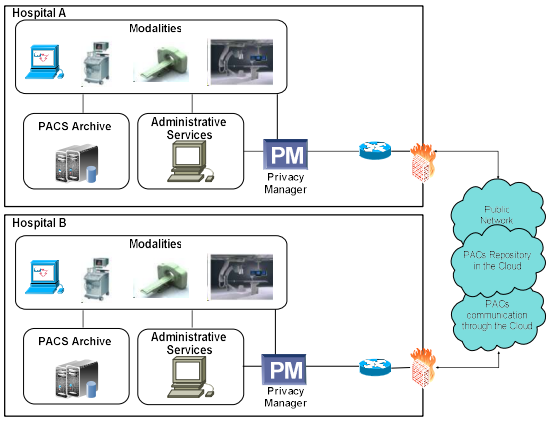

Figure 5 Access anywhere model of the framework

2.2 Experimental Settings

The experiment took place within the main campus of Ladoke Akintola University of Technology, Ogbomoso. Local Area Network Internet connection (LAUnet) available within the campus was used to migrate and retrieve the DICOM Images to and from the cloud. Two computers with similar configurations were used for the experiment. One was used as the workstation that was communicating with the cloud storage services after acquiring the images and accessing them through the developed viewer that was installed on it. The other system served as the local archive server for the traditional PACS that was set up as a benchmark for the Cloud-based PACS archive. The fluctuations in the speed of the Internet connection during the experiment was also recorded. Table 1 shows the pattern of the network while the experiment was being carried out. It is assumed that the Internet network quality in the University is a representation of typical average connectivity strength in the environment of the study.

3. RESULTS AND DISCUSSIONS

The Cloud-PACS security framework was implemented majorly for radiologists and physicians through a DICOM Image System (application). Figure 6 shows the Graphical User Interface for the Cloud-PACS application through which new users can register to successfully login to access the service. As shown in Figure 7, after successfully logging in to the Cloud-PACS application, the uniquely identified user is presented with the available cloud services (Microsoft Azure, Amazon and LAN PACS) so as to make the most preferred choice. An example of the process of setting up one of the cloud service platforms is shown in Figure 8. This is essential so as to enable successful porting of the acquired DICOM images by the application into the preferentially chosen cloud service storage platform. Web services functional invocations required to connect to the cloud is shown in Figure 9. The process of creating the cloud user, its files, registering and accessing the cloud broker service are the major web service functional invocations. The process of obfuscating (securing) the image metadata before migrating into the cloud is shown in Figure 10. The process of appropriately configuring the DICOM images before migrating into the cloud is shown in Figure 11. The DICOM Image System interface which presents operational functionalities for registering for the cloud service and the uploading of the acquired DICOM Images after successful obfuscation is shown in Figure 12.

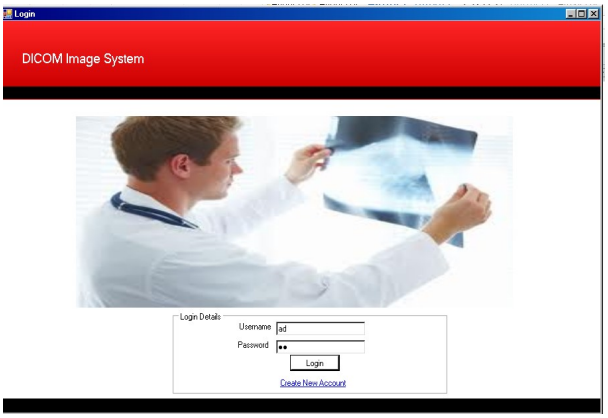

Figure 6: The log-in interface for users into the DICOM Image System

Figure 7: The Cloud Service options available to registered users

Journal of Theoretical and Applied Information Technology
15th April 2019. Vol.97. No 7

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

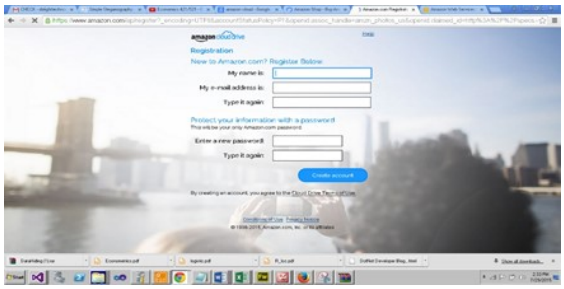

Figure 8: The Amazon Simple Storage Service (sample) cloud platform setup

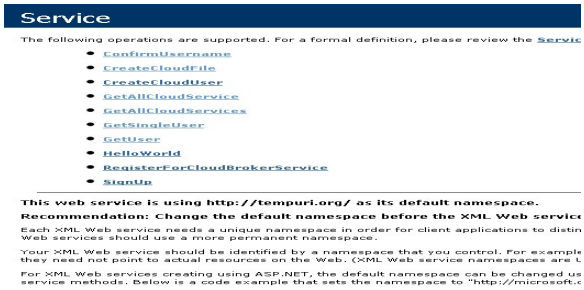

Figure 9: The web service available functional invocations

Figure 10: Image metadata obfuscation in progress

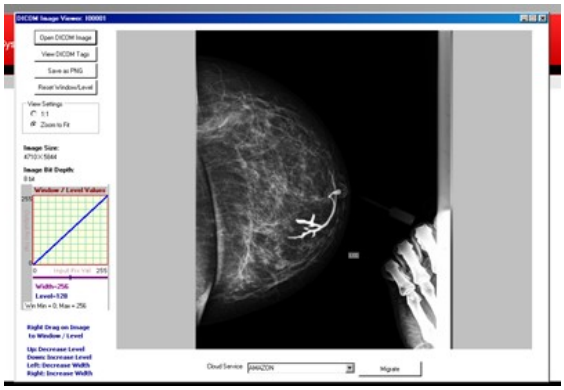

Figure 11: Screenshot showing the process of configuring the DICOM Images

Figure 12: Screenshot of the DICOM Image System operational functionalities

Several uploads and retrieval trials were made on the DICOM Image dataset based on the standard C-STORE and C-MOVE commands. The average time to obtain results with trials is shown in form of tables. Table 2, Table 3, Table 4 and Table 5 display the results for the storage process based on C-STORE for each modality and that of the download process based on C-MOVE. The PACS Cloud storage is a relatively complex process due to the decoupling of the various modules and privacy issues. As expected, the traditional PACS archive image storage, based on DICOM C-STORE command, is faster due to its simplicity and local operations. It is undeniable that cloud storage will be slower than similar operations executed over traditional LAN PACS. However, the important thing is to analyze the solution's feasibility in a real-world environment. The cloud storage time presented is acceptable for a typical DICOM institution, because archiving medical image studies are executed just once and without impacting on the end-user interface.

The analysis of image retrieval time is much more critical to validate the PACS cloud solution because the image data can be accessed (and downloaded) several times in the same procedure and the physician is in front of a work station waiting for the download to be completed. Once again, the traditional PACS image retrieval, based on DICOM C-MOVE command is faster than the Cloud solution. The LAN PACS retrieval delays are similar to storage times because the process time associated with the retrieve command (i.e. C-MOVE) is residual compared to the effective network data transfer (i.e. C-STORE). However, a good observation is that the retrieval time differences from Cloud to LAN are much lower than in the storage process. In general, the experiments show that the solution is robust and that it was possible to store and retrieve all the desired studies without interruptions.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. CONCLUSIONS

The design and implementation of e-health system are increasingly becoming popular in developing countries and security has also been a major point of discussion [22, 23, 24]. Security comes at a great cost at the expense of limited resources [25]. In the field of medical informatics, there are two major computational complexity issues – time and space- that can undermine the widespread use and adoption of a technology. However, PACS technology which has been proven to be useful in this field is subject majorly to the storage computational resource complexity challenge because of the big data inherent in DICOM. Hence, this work proposed and implemented a cloud-based approach for bridging the space complexity gap inherent in PACS-based medical applications. Further, the security of the cloud-plugin to the PACS framework was ensured through the security manager and other complimentary components such as firewall, gateway, and controller. Hence, this framework results in a secure, robust and cost-effective integrated cloud-PACS for the provisioning of medical services. The usability of the proposed framework was enhanced through the cloud-driven technology by mitigating the cost of deployment. Besides using this proposed framework in medical informatics, it can be extended further to electronic commerce and other big data-driven applications. This work is limited in that it did not examine the vulnerabilities of the proposed security framework, future work will consider threat modelling of the developed cloud-PACS to identify the potential security breaches and formulate appropriate mitigation strategies.

REFERENCES:

[1] Huang, H. K. PACS-Based Multimedia Imaging Informatics: Basic Principles and Applications. Wiley-Blackwell, 2019.

[2] Tellis, Wyatt M., Katherine P. Andriole, Christopher S. Jovais, and David E. Avrin. "RIS minus PACS equals film." Journal of digital imaging 15, (2002): 20-26.

[3] Bawack, Ransome Epie, and Jean Robert Kala Kamdjoug. "Adequacy of UTAUT in clinician adoption of health information systems in developing countries: The case of Cameroon." International journal of medical informatics 109 (2018): 15-22

[4] Rehani, Madan M., and Jenia Vassileva. "survey of imaging technology and patient dose recording practice in developing countries." Radiation protection dosimetry, 181, no 3 (2018): 240–245

[5] Silva, Luís A. Bastião, Carlos Costa, and José Luis Oliveira. "DICOM relay over the cloud." International journal of computer assisted radiology and surgery 8, no. 3 (2013): 323-333.

[6] Stergiou, Christos, Kostas E. Psannis, Byung-Gyu Kim, and Brij Gupta. "Secure integration of IoT and cloud computing." Future Generation Computer Systems 78 (2018): 964-975.

[7] Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." (2011): 2 – 3

[8] Wang, Yichuan, LeeAnn Kung, and Terry Anthony Byrd. "Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations." Technological Forecasting and Social Change 126 (2018): 3-13.

[9] Zhao, Fan, Sandra D. Gaw, Nicholas Bender, and Daniel T. Levy. "Exploring Cloud Computing Adoptions in Public Sectors: A Case Study." GSTF Journal on Computing (JoC) 3, no. 1 (2018): 42 – 47

[10] Sharma, Ashish, Tony Pan, B. Barla Cambazoglu, Metin Gurcan, Tahsin Kurc, and Joel Saltz. "VirtualPACS—a federating gateway to access remote image data resources over the grid." Journal of digital imaging 22, no. 1 (2009): 1-10.

[11] Elhoseny, Mohamed, Ahmed Abdelaziz, Ahmed S. Salama, Alaa Mohamed Riad, Khan Muhammad, and Arun Kumar Sangaiah. "A hybrid model of internet of things and cloud computing to manage big data in health services applications." Future generation computer systems 86 (2018): 1383-1394.

[12] Gai, Keke, Meikang Qiu, Hui Zhao, and Xiaotong Sun. "Resource management in sustainable cyber-physical systems using heterogeneous cloud computing." IEEE Transactions on Sustainable Computing 3, no. 2 (2018): 60-72.

[13] Rai, Rashmi, Gadadhar Sahoo, and Shabana Mehfuz. "Exploring the factors influencing the cloud computing adoption: a systematic study on cloud migration." SpringerPlus 4, no. 1 (2015): 197.

[14] Alsmadi, Duha, and Victor Prybutok. "Sharing and storage behavior via cloud computing: Security and privacy in research and practice." Computers in Human Behavior 85 (2018): 218-226.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[15] Kumar, P. Ravi, P. Herbert Raj, and P. Jelciana. "Exploring data security issues and solutions in cloud computing." Procedia Computer Science 125 (2018): 691-697.

[16] Gunadham, Thanyatida, and Pramote Kuacharoen. "Security Concerns in Cloud Computing for Knowledge Management Systems." Journal of Applied Statistics and Information Technology 1, no. 2 (2019): 52-60.

[17] Andry, Francois, Richard Ridolfo, and John Huffman. "Migrating Healthcare Applications to the Cloud through Containerization and Service Brokering." In HEALTHINF, pp. 164-171. 2015.

[18] Löhr, Hans, Ahmad-Reza Sadeghi, and Marcel Winandy. "Securing the e-health cloud." In Proceedings of the 1st ACM International Health Informatics Symposium, pp. 220-229. ACM, 2010.

[19] Maeder, Anthony, and Birgit Planitz. "Cloud-based medical image collection database with automated annotation." (2016): 182-186.

[20] Shahbaz, Sidra, Asiah Mahmood, and Zahid Anwar. "SOAD: Securing oncology EMR by anonymizing DICOM images." In 2013 11th International Conference on Frontiers of Information Technology, pp. 125-130. IEEE, 2013.

[21] Silva, Luís A. Bastião, Carlos Costa, and José Luis Oliveira. "A PACS archive architecture supported on cloud services." International journal of computer assisted radiology and surgery 7, no. 3 (2012): 349-358.

[22] Omotosho, Adebayo, Justice Emuoyibofarhe, and Christoph Meinel. "Ensuring patients' privacy in cryptographic-based-electronic health records using bio-cryptography." International Journal of Electronic Healthcare 9, no. 4 (2017): 227-254.

[23] Omotosho, Adebayo, Justice Emuoyibofarhe, and Alice Oke. "Securing private keys in electronic health records using session-based hierarchical key encryption." Journal of Applied Security Research 12, no. 4 (2017): 463-477.

[24] Omotosho, Adebayo, Justice Emuoyibofarhe, and Christoph Meinel. "Securing E-Prescription from Medical Identity Theft Using Steganography and Antiphishing Techniques." Journal of Applied Security Research 12, no. 3 (2017): 447-461.

[25] Omotosho, Adebayo, and Justice Emuoyibofarhe. "Private key management scheme using image features." Journal of Applied Security Research 10, no. 4 (2015): 543-557.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: Network profile of LAUnet while the experiment was being carried out.

DOWNTIME	DOWNLOAD	UPLOAD
5h49m8s	77.2 MiB	19.4 MiB
1h30m6s	61.5 MiB	3.1 MiB
2h26m41s	56.8 MiB	8.9 MiB
41m2s	1831.7 KiB	195.8 KiB
1h43m35s	36.4 MiB	3.4 MiB
56m43s	44.8 MiB	4.6 MiB
6h55m35s	318.4 MiB	22.3 MiB
14m4s	10.9 MiB	1630.6 KiB
7h46m8s	56.7 MiB	26.8 MiB
1h3m2s	1311.5 KiB	134.1 KiB
1h2m8s	15.1 MiB	2044.5 KiB
55m29s	16.5 MiB	1488.7 KiB
39m19s	987.7 KiB	348.8 KiB
3h31m8s	376.0 MiB	15.8 MiB
1h7m59s	5.1 MiB	418.2 KiB
8h31m24s	285.7 MiB	37.6 MiB
29m54s	43.6 MiB	2.5 MiB
51m11s	1291.4 KiB	237.8 KiB
2h2m30s	141.2 MiB	8.3 MiB
9h13m31s	111.7 MiB	28.5 MiB
3h50m	532.5 MiB	37.5 MiB
2h17m16s	42.2 MiB	6.3 MiB
4h2m17s	10.1 MiB	21.9 MiB
2h50m8s	845.4 MiB	88.2 MiB
3h47m48s	81.7 MiB	6.4 MiB
2h18m41s	39.9 MiB	8.9 MiB
1h4m36s	552.9 KiB	158.1 KiB
8h23m55s	84.8 MiB	21.6 MiB
35s	133.5 KiB	119.5 KiB
2h50m37s	224.5 MiB	17.1 MiB
2h48m20s	84.1 MiB	7.2 MiB
49m16s	13.4 MiB	1077.4 KiB
3h10m17s	56.0 MiB	47.5 MiB
1h17m6s	12.2 MiB	2.3 MiB
3h34m21s	2.1 GiB	56.0 MiB
1h2m37s	1718.8 KiB	368.2 KiB
56m48s	24.9 MiB	3.8 MiB
32m23s	412.5 KiB	121.9 KiB
1h46m48s	42.6 MiB	5.0 MiB
34m57s	5.1 MiB	1621.9 KiB

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2: Average access time for Computed Tomography Images

		C-STORE			C-MOVE		
Number of Files	Average File Size (MB)	Average Time Azure (sec)	Average Time Amazon S3 (sec)	Average Time LAN PACS (sec)	Average Time Azure (sec)	Average Time Amazon S3 (sec)	Average Time LAN PACS (sec)
12	20	10.55	10.81	6.23	6.55	5.12	4.22
24	18.5	10.4	10.09	5.91	5.78	6.23	5.2
23	15	9.75	9.6	5.33	3.94	4.32	3.2
31	13.2	9.12	9.35	3.98	5.08	5.29	4.6
11	12.7	8.68	8.81	4.34	6.43	5.26	4.08
23	10.56	8.39	8.23	4.9	5.19	4.65	3.89
11	9	7.86	8.02	2.45	4.18	5.24	3.55
17	8.15	7.32	7.75	3.72	3.97	3.32	2.56
22	5.3	6.78	6.56	2.12	4.8	3.87	2.79
42	4.4	5.87	5.71	5.01	6.91	5.64	3.06

Table 3: Average access time for Digital Radiography (DX) Images.

		C-STORE			C-MOVE		
Number of Files	Average File Size (MB)	Average Time Azure (sec)	Average Time Amazon S3 (sec)	Average Time LAN PACS (sec)	Average Time Azure (sec)	Average Time Amazon S3 (sec)	Average Time LAN PACS (sec)
15	20	10.56	10.12	7.34	9.76	8.51	7.43
41	18.5	9.23	8.98	5.32	8.7	9.23	7.39
38	15	8.35	8.75	4.99	8.43	8.21	7.17
20	13.2	7.45	7.79	3.01	7.65	8.09	6.87
11	12.7	7.01	6.87	3.23	7.21	7.43	6.31
49	10.56	6.23	6.56	4.19	6.87	6.98	6.01
43	9	6.19	6.05	2.03	6.32	5.91	5.21
41	8.15	5.45	5.59	4.96	5.54	5.24	4.82
38	5.3	4.78	4.65	4.21	5.02	4.86	4.13
100	4.4	3.73	3.86	3.13	4.76	4.2	3.87

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 4: Average access time for Nuclear Medicine (NM) Images.

		C-STORE			C-MOVE		
Number of Files	Average File Size (MB)	Average Time Azure (sec)	Average Time Amazon S3 (sec)	Average Time LAN PACS (sec)	Average Time Azure (sec)	Average Time Amazon S3 (sec)	Average Time LAN PACS (sec)
12	20	9.82	9.76	9.32	9.54	8.76	8.3
19	18.5	9.23	8.95	8.65	8.01	8.32	7.76
10	15	8.73	8.43	8.01	7.76	7.91	7.23
42	13.2	7.45	7.78	6.84	6.98	7.21	6.5
14	12.7	7.05	7.23	6.58	6.8	6.76	6.13
31	10.56	6.77	6.4	5.8	6.12	5.98	5.76
18	9	6.13	5.76	5.15	5.45	5.32	4.56
27	8.15	5.45	5.65	4.35	4.79	4.67	3.8
65	5.3	5.55	5.13	4.85	4.21	3.87	3.12
63	4.4	4.91	4.87	4.12	3.35	3.6	2.87

Table 5: Average access time for X-ray Angiography (XA) Images

		C-STORE			C-MOVE		
Number of Files	Average File Size (MB)	Average Time Azure (sec)	Average Time Amazon S3 (sec)	Average Time LAN PACS (sec)	Average Time Azure (sec)	Average Time Amazon S3 (sec)	Average Time LAN PACS (sec)
52	20	9.65	9.76	5.01	6.55	5.12	4.22
55	18.5	9.34	9.13	4.84	5.78	6.23	5.2
39	15	8.97	8.67	4.43	3.94	4.32	3.2
51	13.2	8.01	8.23	4.9	5.08	5.29	4.6
35	12.7	7.72	7.81	3.34	6.43	5.26	4.08
20	10.56	7.13	7.34	3.78	5.19	4.65	3.89
44	9	6.87	6.76	3.37	4.18	5.24	3.55
21	8.15	6.12	6.23	2.89	3.97	3.32	2.56
53	5.3	5.76	5.9	2.23	4.8	3.87	2.79
232	4.4	4.91	5.17	1.35	6.91	5.64	3.06