A Dynamic Cloud Computing Platform for eHealth Systems

Mehdi Bahrami [1] and Mukesh Singhal [2]

Cloud Lab
University of California Merced, USA
Email: [1] IEEE Senior Member, MBahrami@UCMerced.edu; [2] IEEE Fellow, MSinghal@UCMerced.edu

***Abstract*— Cloud Computing technology offers new opportunities for outsourcing data, and outsourcing computation to individuals, start-up businesses, and corporations in health care. Although cloud computing paradigm provides interesting, and cost effective opportunities to the users, it is not mature, and using the cloud introduces new obstacles to users. For instance, vendor lock-in issue that causes a healthcare system rely on a cloud vendor infrastructure, and it does not allow the system to easily transit from one vendor to another. Cloud data privacy is another issue and data privacy could be violated due to outsourcing data to a cloud computing system, in particular for a healthcare system that archives and processes sensitive data. In this paper, we present a novel cloud computing platform based on a Service-Oriented cloud architecture. The proposed platform can be ran on the top of heterogeneous cloud computing systems that provides standard, dynamic and customizable services for eHealth systems. The proposed platform allows heterogeneous clouds provide a uniform service interface for eHealth systems that enable users to freely transfer their data and application from one vendor to another with minimal modifications. We implement the proposed platform for an eHealth system that maintains patients' data privacy in the cloud. We consider a data accessibility scenario with implementing two methods, AES and a light-weight data privacy method to protect patients' data privacy on the proposed platform. We assess the performance and the scalability of the implemented platform for a massive electronic medical record. The experimental results show that the proposed platform have not introduce additional overheads when we run data privacy protection methods on the proposed platform.**

Keywords— Cloud Computing; Data Security; Data Privacy; eHealth Platform; Dynamic Cloud Computing Architecture;

I. INTRODUCTION

Cloud computing offers a new technology to multidiscipline fields to establish a virtual IT department via the Internet [1, 2]. The cloud computing offers different virtual services like traditional IT department, such as storage, stream server and database server. The cloud provides a cost effective model through pay-per-use that allows each individual or businesses in healthcare start a cloud based service with minimum investment [1, 2]. However, the cloud computing has several major issues [1, 3, 4, 5] for an eHealth system which are discussed as follows.

Migration Issue: Data and application migration is one of the major issues when users decide to transfer their data and applications from an IT department to a cloud computing system or from one cloud computing to another. Migration may causes several sub-issues, such as data security issue. For instance, a user who used a regular application based on a specific Application Programming Interface (*API*) could have some issue when the application transfer to a cloud computing system that needs to redefine or modify the security functions of the API in order to use the cloud. Each cloud computing system offer own services to

Security Issue: Data security refers to accessibility of stored data to only authorized users, and network security refers to accessibility of transfer of data between two authorized users through a network. Since cloud computing uses the Internet as part of its infrastructure, stored data on a cloud is vulnerable to both a breach in data and network security.

Data Privacy: Users have to outsource their data to an untrusted cloud vendor (e.g., public cloud vendors) in order to use the cloud computing benefits. In addition of data and network hack issues in cloud computing, data privacy could be violated by other users, malicious applications or even the cloud vendor when users share their data with a cloud vendor. Data privacy becomes one of the major challenges in outsourcing data to the cloud. Data encryption methods allow users to avoid exposing the original data to the cloud vendors. However, encryption for each single original data is not cost effective or feasible for some machines, such as mobile devices. For example, some mobile devices in eHealth systems have limited resources, such as *CPU*, *RAM* and battery power.

II. BACKGROUND

In our previous study, we developed a dynamic cloud computing architecture based on Service-Oriented Architecture (*DCCSOA*) [4]. The architecture provides a new layer, *Template-as-a-Service (TaaS)*, on the top of a cloud computing system that allows a cloud vendor to standardize its cloud services by defining *TaaS* services. *TaaS* is divided into two sub-layers: *front-end (FTaaS)* that allows different cloud vendors to define a generic and standard cloud service, and *back-end (BTaaS)* that allows a cloud vendor to bind a defined generic cloud service, *FTaaS*, to its cloud computing system. In other words, *DCCSOA* enables different cloud vendors to standardize their services through a uniform interface at *FTaaS* that allows users to transfer their data and applications from one vendor to another.

In this paper, we use *DCCSOA* to provide a *template*, *TaaS*, for eHealth system. A *template* allows an eHealth system to use heterogeneous cloud computing systems. It provides flexibility, customizability and standardization for eHealth services that needs to be run on the cloud computing.

As previously discussed, the data security and data privacy are two major issues in cloud computing system for eHealth

978-1-4673-8325-7/15/$31.00 ©2015 IEEE

systems. We will use a light-weight data privacy method (*DPM*) [6] that allows clients to scramble the original data on the client side before submitting to the cloud, and AES encryption method on the proposed platform. We evaluate the performance of implemented platform while clients use the methods.

Our contribution in this paper are as follows:

- Propose a platform for eHealth system based on *DCCSOA*.
- Introduce an *eHealth template* for the proposed platform that provides a uniform interface for eHealth systems to interact with heterogeneous cloud computing systems.
- Conduct an experiment through *DPM* and AES on the proposed platform to evaluate the performance and scalability of the proposed platform.

The rest of the paper is organized as follows: In the next section, we introduce the proposed platform based on *DCCSOA*. We discuss the implementation of the proposed platform in section IV. We evaluate the behavior of *DPM* and AES on the proposed platform for a massive healthcare dataset in Section V. We review related work in Section VI, and finally, we conclude our study in Section VII.

III. The Proposed Platform

We consider *DCCOSA* as the main architecture for the proposed cloud platform. We define an *eHealth Template*, (T_{eH}), for eHealth systems which is divided into the front-end, $FTaaS_{eH}$, and the back-end, $BTaaS_{eH}$.

$FTaaS_{eH}$ provides a generic and a uniform interface with standard services. $BTaaS_{eH}$ binds specific cloud value-added services to the uniform service interfaces at $FTaaS_{eH}$.

Figure 1 illustrates a general view of cloud stacks for the proposed platform. A client (end-user) accesses a generic and a uniform cloud service interfaces through an *eHealth Client Application*. The proposed platform can be simply transferred from a vendor V_1 to another V_2 by using the same $FTaaS_{eH}$ in another cloud but with different $BTaaS_{eH}$.

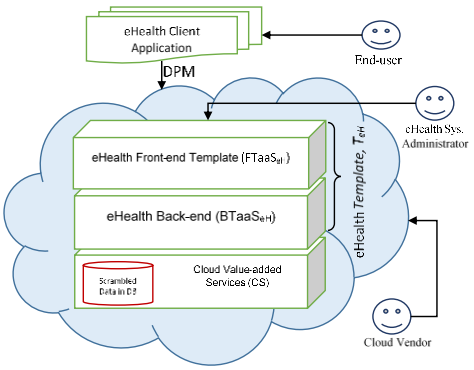


Figure 1. A view of eHealth template with implementation of DPM and its connection to cloud value-added services

$FTaaS_{eH}$ is a dynamic layer, and it allows cloud vendors to customize their cloud services as *a template*. First, cloud vendors bind defined generic and uniform services at $FTaaS_{eH}$ to their value-added services through $BTaaS_{eH}$. As shown in Equation 1 each service at $FTaaS_{eH}$ must pass a satisfaction function $\mathcal{S}$ to propose a uniform service interface.

$$\exists\, s \in FTaaS_{eH} \mid \mathcal{S}at(s) \quad (1)$$

where s is a service at $FTaaS_{eH}$ and $\mathcal{S}at$ is a satisfaction function which is defined as follows:

$$Sat(s): \mathcal{R} \rightarrow \mathcal{O} \quad (2)$$

where $\mathcal{R}$ is a finite set of requirements of r, and $\mathcal{O}$ is a finite set of corresponding output for each requirement in $\mathcal{R}$.

The uniform service interface, UI, can be defined as follows:

$$UI(s) \rightarrow Sat(s_1)\hat{}Sat(s_1)\hat{}..Sat(s_k) \quad (3)$$

Code I shows an example of how a client accesses *FTaaS* through a uniform data access layer with an abstraction on a cloud service (database access in this case). In this code, a client loads a web service, *FTaaS_Service_Ref*, for accessing services on the proposed platform. Then, the client requests a data access by calling *GetDataList* procedure from the web service, and finally, it retrieves the result on an object, *DataGridView*.

Code I. Data Access at client side through *FTaaS*

```
FTaaS_Service_Ref.Service1Client FTS
=new FTaaS_Service_Ref.Service1Client();
DataSet ds = FTS.GetDataList();
DataGridView.DataSource = ds.Tables[0];
DataGridView.DataBind();
```

On one hand, defined services at *FTaaS* are dynamic, and the services can be customized by a cloud vendor to provide different type of services to the clients. Cloud vendors bind services from *BTaaS* to their value-added cloud services that facilitates a service accessibility on heterogeneous cloud services for an eHealth system. On the other hand, an eHealth application, and its data can be transferred to another cloud vendor with minimal modifications at the client side. In addition, providing a generic and a uniform service is important for mobile health care devices because software modification for these devices can be expensive, and sometime requires hardware modifications.

IV. Experimental Setup

We implemented the proposed platform through a case study based on a defined *template* for an eHealth system. The proposed platform provides a generic data access at *FTaaS* to end-users for accessing to an *Electronic Medical Record (EMR)*. We implemented two methods on the proposed platform to protect patients' data privacy - one is a light-weight data privacy method (*DPM*) which is described in [6] and [7] and another method is AES encryption [8]. These methods allows us to assess the performance of the proposed platform.

We consider the following scenario for the implementation of the proposed platform.

"A client requests a data access to an Electronic Medical Record (EMR) which is implemented as a web service at FTaaS. FTaaS provides a generic, and a uniform function to the client. The request will be submitted from FTaaS to the BTaaS. Each

retrieved response is processed through two user-data protection methods, DPM and AES encryption. BTaaS is implemented by Windows Communication Foundation (WCF) [9], and it is bounded to a SQL database. We ran different queries at this level, and uses data protection methods to evaluate the performance of the proposed platform. BTaaS' responses sent to the client at FTaaS by a web service."

We implemented the proposed platform that includes an *eHealth template*. The *template* at the *FTaaS* enables end-users to interact with data access layer without considering the source of data. In the proposed platform is *FTaaS* and *BTaaS* are implemented as a web service, a *Windows Communication Foundation (WCF)* service, respectively. The services can be easily customized at *BTaaS* to adapt with heterogeneous cloud computing systems or traditional IT systems.

We used an Artificial Large Medical Dataset[1] as our *EMR* database that contains records of 100,000 *patients*, 361,760 *admissions*, 107,535,387 *lab observations*, and with the size of 12,494,912 KB (~12.2 GB). We ran 31 different queries on the largest table, *lab observations*. Each query retrieved different numbers of fields with different size. We ran *DPM* and *AES Encryption* at *BTaaS* to protect patients' data privacy on each retrieved field. It allows us to assess the performance of the methods on the proposed platform by monitoring the computation time of the methods for each retrieved field from database.

The processed queries in this experiment are based on *Select Distinct Top* in *TSQL* language that retrieves data from 6 fields to 30,000 fields with the total queries' result size from 180 Byte to 911 Mbyte.

In this paper, we are interested in evaluation of both *quantity parameters* and *quality parameters* in the proposed platform.

The *quantity parameters* includes the following parameters:

Performance: We consider different workloads to evaluate the performance of a given method on the proposed platform and its performance when the size of workload is increased.

Scalability: A scalable service allows the service to provide the same performance when the number of transactions is increased.

The *quality parameters* includes the following parameters:

Customization: The higher level of this parameter allows a cloud vendor to customize provided *services* with minimum modifications.

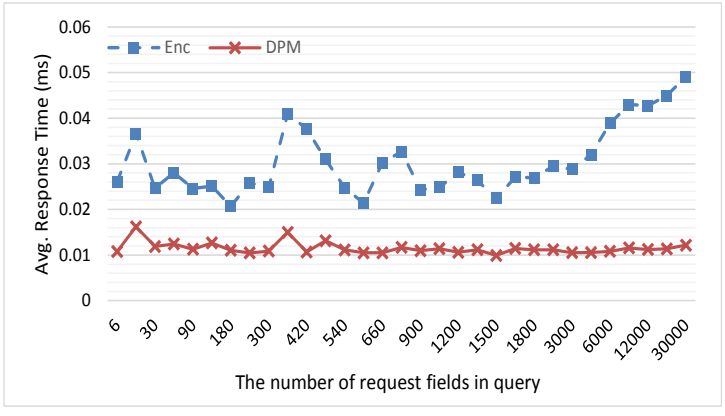
Independence of services: The higher level of this parameter allows the administrator to freely transfer an eHealth system to another cloud vendor or bring it back to a traditional IT department with minimal service modifications.

Standardization of service: The higher level of this parameter allows an eHealth system to interact with heterogeneous cloud services with minimal modifications.

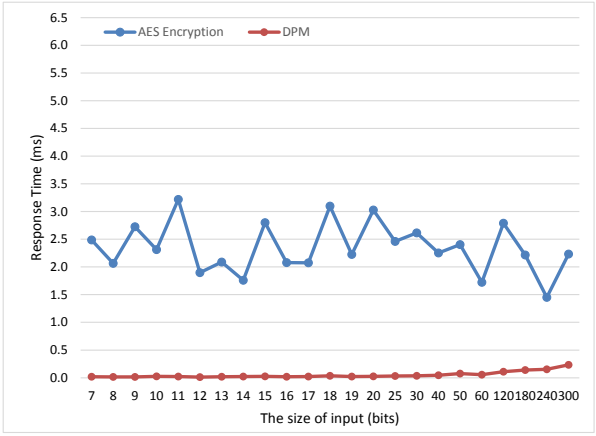
V. Experimental Results

Figure 2 illustrates the experimental results for the evaluation of the quantity parameters on the proposed platform for an eHealth system. We ran 31 different queries on the *EMR* database. Each submitted query from *FTaaS* is processed on the proposed platform to retrieve data from database at *BTaaS*. The platform is retrieved the response of each query and ran *DPM* and *AES* encryption on each retrieved field (result) from *BTaaS*. Figure 2.a shows the performance of the implemented methods on the proposed platform.

We expect that *DPM* provide a better performance over *AES* as described in [8] as well as on the proposed platform. Figure 2.a compares the performance of *DPM* and *AES* encryption on the proposed platform. This figure shows that *DPM* provides a better performance over *AES* encryption for all query results as we expected.



(a) A comparision between the performance of DPM and AES on the proposed platform



(b) A comparision between the performance of DPM and AES for a single Unicode string with different sizes

Figure 2. Experimental Results

[1] http://www.emrbots.org retrieved on July 12, 2015

Figure 2.b illustrates the performance of *DPM* and *AES* encryption for different size of an input string while the methods are not performed on the proposed platform. We considered each input string as a Unicode character with a size of 16 bits each. X-axis represents the size of input string, and Y-axis represents its response time (millisecond). In our experiment, we assumed that *DPM* does not need to generate a set of *PRP* by accessing to predefined arrays that described in [6].

Figures 2.a and 2.b show that the performance of processing of *DPM* and *AES* on the proposed platform (Figure 2.a) is not different from a single string (in Figure 2.b).

Another parameter which can be evaluated is quality parameters that includes *service independency* and a *service standardization*.

As described in Code I, a client can access the platform by using the provided generic service. Since the service is independent of the cloud value-added services at the *BTaaS*, it allows users to interact with the cloud services without concerning about its requirements or type of output of a service. For instance, an application at client side in Scenario 1 retrieves data without understanding the type of database, and the location of the database. The service at *FTaaS* can be bind to any kind of services at *BTaaS*.

Different cloud vendors are able to define the similar services at *FTaaS* in Scenario I that allows an eHealth system use different cloud standardized services.

VI. Related Work

Several cloud-based services and platforms have been developed for eHealth systems. For instance, Fan et al. [10] developed a platform which is used from capturing health care data for processing on the cloud computing. The platform relies on its architecture, and the authors did not describe how the proposed platform can be implemented for different architectures or how it can customize services for heterogeneous clouds. As discussed previously, a dynamic and a customizable cloud platform allows administrators to implement, and to transfer an eHealth system to different cloud computing systems. There is also a vendor lock-in issue [5], if a platform's services rely on a specific cloud architecture. In another study, Lounis et al. [11] developed a secure cloud architecture which is only focused on wireless sensor networks, and the study has limited work on the architecture. The study does not discussed the architecture features, such as service modifications or dynamic services. Magableh et al. [12] proposed a dynamic rule-based approach without considering the cloud environment. Finally, Hoang et al. [13] focus on mobile users features in their proposed architecture, and the study does not discuss the overall of the architecture. In our study, we proposed a dynamic platform for eHealth system, and we showed how the proposed platform implements a dynamic service at *FTaaS*.

VII. Conclusion

In this paper, we proposed a dynamic cloud platform for an eHealth system based on a cloud *SOA* architecture, *DCCSOA*. The proposed platform can be run on the top of heterogeneous cloud computing systems that allows a cloud vendor to customize and standardize services with minimal modifications. The platform uses a *template* layer which is divided into *FTaaS* that allows cloud vendors to define a standard, generic, and uniform service, and *BTaaS* that allows defined services at *BTaaS* to bind to the cloud vendor value-added services. In addition, we implemented a data access scenario on the proposed platform with two different methods to evaluate its performance. The first method is a light-weight data privacy method (*DPM*), and the second is *AES* encryption method. The evaluation shows that the platform is scalable and the methods which are ran on the platform have not introduce additional overheads.

References

[1] Rodrigues, Joel JPC, ed. "Health Information Systems: Concepts, Methodologies, Tools, and Applications", Vol. 1. IGI Global, 2009.

[2] Mehdi Bahrami and Mukesh Singhal, "The Role of Cloud Computing Architecture in Big Data", Information Granularity, Big Data, and Computational Intelligence, Vol. 8, pp. 275-295, Chapter 13, Pedrycz and S.-M. Chen (eds.), Springer, 2015 http://goo.gl/4gNW3s

[3] Landau, Susan. "Highlights from Making Sense of Snowden, Part II: What's Significant in the NSA Revelations" Security & Privacy, IEEE 12.1 (2014): 62-64.

[4] Mehdi Bahrami and Mukesh Singhal, "DCCSOA: A Dynamic Cloud Computing Service-Oriented Architecture", IEEE International Conference on Information Reuse and Integration (IEEE IRI'15), San Francisco, CA, USA. Aug 2015.

[5] Kumar, Karthik, and Yung-Hsiang Lu. "Cloud computing for mobile users: Can offloading computation save energy?" Computer 43.4 (2010): 51-56.

[6] Mehdi Bahrami and Mukesh Singhal, "A Light-Weight Permutation based Method for Data Privacy in Mobile Cloud Computing" in 3rd Int. Conf. IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (IEEE Mobile Cloud 2015) San Francisco, IEEE, 2015.

[7] Bahrami, Mehdi. "Cloud Computing for Emerging Mobile Cloud Apps" Mobile Cloud Computing, Services, and Engineering (MobileCloud), 3rd IEEE International Conference on. 2015.

[8] Harrison, Owen, and John Waldron, "AES encryption implementation and analysis on commodity graphics processing units", Springer Berlin Heidelberg, 2007.

[9] Resnick, Steve, Richard Crane, and Chris Bowen, "Essential windows communication foundation: for .Net framework 3.5", Addison-Wesley Professional, 2008.

[10] Fan, Lu, et al. "DACAR platform for eHealth services cloud." Cloud Computing (CLOUD), 2011 IEEE International Conference on. IEEE, 2011.

[11] Lounis, Ahmed, et al. "Secure and scalable cloud-based architecture for e-health wireless sensor networks." Computer communications and networks (ICCCN), 2012 21st international conference on. IEEE, 2012.

[12] Magableh, Basel, and Michela Bertolotto, "A Dynamic Rule-based Approach for Self-adaptive Map Personalisation Services", International Journal of Soft Computing and Software Engineering (JSCSE), vol.3. no.3, 104, March 2013.

[13] Hoang, Doan B., and Lingfeng Chen. "Mobile cloud for assistive healthcare (MoCAsH)" Services Computing Conference (APSCC), 2010 IEEE Asia-Pacific. IEEE, 2010