JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 09, ISSUE 01, 2022

eHealth Systems on a Dynamic Cloud Computing Platform

Mrs.T.Swathi, Assistant Professor, Department of Information Technology, CMR Engineering College, Hyderabad, Telangana,
E-Mail-id swathi.tamma@cmrec.ac.in

Mrs.C.Madhuri, Assistant Professor, Department of Information Technology, CMR Engineering College, Hyderabad, Telangana,
E-Mail-id madhurichinnam@cmrec.ac.in

ABSTRACT
The development of cloud computing has opened up new possibilities for individuals, small enterprises, and large corporations in the healthcare industry to outsource computation and data. Although the cloud computing paradigm offers users exciting and cost-effective alternatives, it is still in its infancy and using the cloud presents users with new challenges. For instance, a vendor lock-in problem makes a healthcare system dependent on a cloud vendor infrastructure and makes it difficult for the system to switch vendors quickly. Another issue is cloud data privacy, which can be compromised when data is outsourced to a cloud computing system, particularly in the case of healthcare systems that store and handle sensitive patient data. Using a service-oriented cloud architecture, we introduce an unique cloud computing platform in this work. The suggested platform can be used on top of many cloud computing platforms that offer eHealth systems with standardized, adaptable, and dynamic services. The suggested platform enables users to freely move their data and applications from one vendor to another with little to no modification. Heterogeneous clouds are able to provide a uniform service interface for eHealth systems. We put into practise the suggested platform for an eHealth setup that protects patient data privacy in the cloud. In order to safeguard the privacy of patient data on the suggested platform, we take into account a data accessibility situation with the implementation of two methods: AES and a lightweight data privacy approach. We evaluate the platform's scalability and performance for a sizable electronic medical record. The experimental results demonstrate that when we run data privacy protection algorithms on the suggested platform, no additional overheads are introduced.

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

INTRODUCTION
By using the Internet to create a virtual IT department, cloud computing provides multidisciplinary fields with new technology [1, 2]. Similar to a traditional IT department, the cloud offers a variety of virtual services like storage, stream servers, and database servers. Pay-per-use models offered by the cloud enable individuals or organizations in the healthcare industry to launch cloud-based services with a minimal outlay of capital [1, 2]. However, there are a number of significant problems with cloud computing [1, 3, 4, 5] that are explored here with regard to an eHealth system.

When customers choose to move their data and apps from an IT department to a cloud computing system or from one cloud

computing to another, there are significant difficulties. Data security is one of the many subproblems that migration may bring about. For instance, when an application is transferred to a cloud computing system and the security functions of the API need to be redefined or modified in order to use the cloud, a user of the regular application that was based on the specific Application Programming Interface (API) may experience some problems. Every cloud computing platform provides unique features to Security Issue: Network security refers to the ability to transfer data between two authorized users through a network, whereas data security refers to the accessibility of stored data to only authorized users. Data stored on a cloud is susceptible to both a data security breach and a network security breach since cloud computing employs the Internet as part of its infrastructure.

Data Privacy: To take use of the advantages of cloud computing, users must outsource their data to an unreliable cloud vendor (such as a public cloud vendor).When consumers share their data with a cloud provider, data privacy may also be breached by other users, malicious programmers, or even the cloud vendor. This is in addition to difficulties with data and network hacks in cloud computing. One of the biggest problems with outsourcing data to the cloud is data protection. Users can prevent disclosing the original data to cloud vendors by using data encryption technologies. For some computers, such as mobile devices, encryption for every single original piece of data is neither practical nor cost-effective. For instance, several mobile devices used in eHealth systems have constrained CPU, Memory, and battery life.

I. BACKGROUND

We created a dynamic cloud computing architecture (DCCSOA) based on service-oriented architecture in our prior study [4]. The design adds a new layer called Template-as-a-Service (TaaS) on top of a cloud computing system that enables a cloud vendor to define TaaS services to standardize their cloud services. TaaS has two sublayers: the front-end (FTaaS), which enables various cloud vendors to create a general and standard cloud service, and the back-end (BTaaS), which enables a cloud vendor to link a defined generic cloud service, FTaaS, to its cloud computing system. In other words, DCCSOA lets users to move their data and apps between cloud vendors by providing a consistent interface at FTaaS that enables different cloud vendors to standardize their services.

In this article, we use the DCCSOA to offer a TaaS template for an eHealth system. An eHealth system can employ many cloud computing platforms thanks to a template. For eHealth services that must be run on cloud computing, it offers flexibility, customizability, and standardization.

As was already said, there are two key concerns with cloud computing for e Health systems: data security and data privacy. We'll employ AES encryption on the suggested platform together with a light-weight data privacy method (DPM) [6] that enables clients to scramble the original data on the client side before submitting to the cloud. While clients are utilising the approaches, we assess the platform's performance.

Following are the contributions we made to this paper:

- Create an eHealth system platform based on DCCSOA.
- Provide an eHealth template for the suggested platform that gives eHealth systems a consistent interface to communicate with diverse cloud computing platforms.
- Conduct an experiment through DPM and AES on the proposed platform to evaluate

the performance and scalability of the proposed platform. The remainder of the essay is structured as follows: We introduce the suggested platform based on DCCSOA in the following section. In section IV, we go over how the suggested platform will be put into practise. In Section V, we assess how DPM and AES behave on the suggested platform for a sizable healthcare dataset.In Section VI, we evaluate related literature, and in Section VII, we draw a conclusion to our investigation.

II. THE PROPOSED PLATFORM

DCCOSA is what we view as the primary architecture for the suggested cloud platform. For eHealth systems, we create an eHealth Template (TeH), which is split into the front-end (FTaaSeH) and back-end (BTaaSeH).

A unified and generic interface with common services is offered by FTaaSeH. Certain cloud value-added services are bound to the standardised service interfaces at FTaaSeH by BTaaSeH.

A general picture of the cloud stacks for the suggested platform is shown in Figure 1. A client (end user) uses an eHealth Client Application to access a standard and generic cloud service interface.By using the same FTaaSeH in a separate cloud with a different BTaaSeH, the suggested platform can be easily switched from one vendor V1 to another V2 without any additional effort.

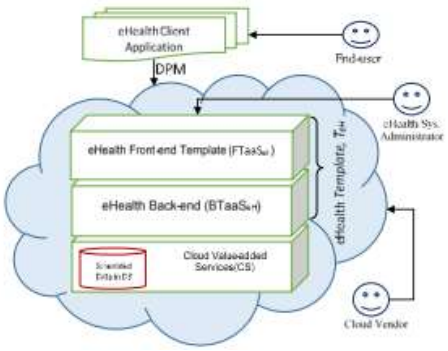

Figure 1 shows how the eHealth template looks with DPM implemented and connected to cloud value-added services.

Being a dynamic layer, FTaaSeH enables cloud vendors to personalise their cloud services using it as a model. First, cloud vendors tie their value-added services through BTaaSeH to defined generic and uniform services at FTaaSeH. According to Equation 1 each service at FTaaseH must pass a satisfaction function detla to propose a uniform service interface.

$$\exists\, s \in FTaaS_{eH} \mid Sat(s) \qquad (1)$$

where s is a service at FTaaseH is a satisfaction function which is defined as follows:

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

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

It is possible to define the uniform service interface like follows:

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

Code I provide an illustration of how a client can use a cloud service's consistent data access layer to access FTaaS. (database access in this case). A client loads the web service FTaaS Service Ref in this code to access the services on the suggested platform. The client then makes a request to the web service to get data by calling the GetDataList function, and then it retrieves the data on an object called 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();
```

ISSN- 2394-5125 VOL 09, ISSUE 01, 2022

On the one hand, specified services in FTaaS are dynamic and may be tailored by a cloud vendor to offer clients various types of services. In order to simplify service accessibility on heterogeneous cloud services for an eHealth system, cloud vendors tie BTaaS services to their value-added cloud services. Yet, an eHealth application and its data can be moved to another cloud provider with little client-side modification. Furthermore, because it can be costly and occasionally necessitates hardware modifications, it is crucial to offer a generic and uniform service for mobile health care equipment.

III. EXPERIMENTAL SETUP

Based on a predetermined design for an eHealth system, we put the suggested platform into practice through a case study. The suggested platform offers end users a general data access at FTaaS for obtaining an electronic medical record (EMR).In order to secure the privacy of patient data, we implemented two approaches on the suggested platform: one is a light-weight data privacy method (DPM), which is described in [6] and [7], and the other is AES encryption [8]. We can evaluate the performance of the suggested platform using these techniques.

For the implementation of the suggested platform, we take into account the following scenario.

"An electronic medical record (EMR) that is implemented at FTaaS as a web service is the subject of a client request for data access. The client receives a generic and consistent service from FTaaS. The FTaaS will make the request to the BTaaS. Per Code I. Client-side Data Access through FTaaS FTaaS Service Ref.Service1Client DataSet ds = FTS.GetDataList(); DataGridView.DataSource = ds.Tables[0]; DataGridView.DataBind(); Figure 1; FTS =new FTaaS Service Ref.Service1Client();DPM and AES encryption are used to process a view of an eHealth template with DPM implementation and its link to cloud value-added services received response. Windows Communication Framework (WCF) [9] implements BTaaS, which is connected to a SQL database. We used data protection techniques and various queries to assess the performance of the suggested platform at this level. Responses from BTaaS are transmitted over a web service to the client at FTaaS.

We put into practice the suggested platform, which has an eHealth template. The FTaaS template allows end users to interact with the data access layer without taking into account the source of the data..FTaaS and BTaaS are implemented in the suggested platform as web services and Windows Communication Foundation (WCF) services, respectively. With BTaaS, the services can be easily adjusted to fit with either traditional IT systems or heterogeneous cloud computing platforms. As our EMR database, we selected an Artificial Big Medical Dataset1 that has records for 100,000 patients, 361,760 admissions, 107,535,387 lab observations, and is around 12.2 GB in size. The largest table, lab observations, was subjected to 31 separate queries. Every query produced a varied number of fields of varying sizes. To safeguard the privacy of patients' data on each retrieved field, DPM and AES encryption were used at BTaaS. By tracking the computation times of the techniques for each retrieved field from the database, it enables us to evaluate the effectiveness of the methods on the suggested platform. The processed Choose Distinct Top queries used in this experiment retrieve data from 6 to 30,000 fields with total query result sizes ranging from 180 bytes to 911 Mbytes. We are interested in evaluating the quality and

quantity parameters in the suggested platform in this work.

The following parameters are part of the quantity parameters:0

Performance: To assess a method's performance on the suggested platform and its performance as the workload size is increased, we take into account various workloads.

Scalability: When a service is scalable, it may continue to deliver the same level of performance even if the volume of transactions rises.

The quality parameters includes the following parameters:

Customization: The more advanced level of this parameter enables a cloud vendor to modify the services offered with few changes.

Independence of services: The higher level of this parameter enables the administrator to easily return an eHealth system to a traditional IT department or freely transfer it to another cloud provider with only minor service modifications.

Standardization of service: The greater level of this parameter enables minimally modified interaction between an eHealth system and diverse cloud services.

IV. EXPERIMENTAL RESULTS

The experimental findings for the assessment of the quantity parameters on the suggested platform for an eHealth system are shown in Figure 2. On the EMR database, we executed 31 separate queries. Each request made by FTaaS is processed on the suggested platform in order to retrieve information from the BTaaS database. The platform downloaded each query's response from BTaaS and then executed DPM and AES encryption on each field (result).The effectiveness of the strategies put into practice on the suggested platform is shown in Figure 2.a.

We anticipate that DPM will perform better than AES on both the suggested platform and as stated in [8].The effectiveness of DPM and AES encryption on the suggested platform is contrasted in Figure 2.a. This graph demonstrates that, as we anticipated, DPM offers superior speed to AES encryption for all query results.

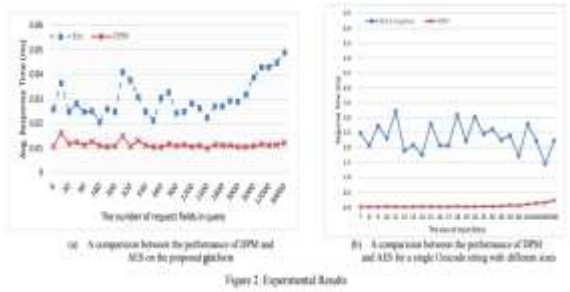

Figure 2.b shows how DPM and AES encryption work for input strings of various sizes when the methods are not used on the suggested platform. Each input string was treated as a single Unicode character with a size of 16 bits. The input string's size is shown on the X-axis, while its response time is shown on the Y-axis (millisecond).In our experiment, we made the supposition that DPM doesn't necessarily need to construct a set of PRP by accessing the preset arrays specified in [6].

Figures 2.a and 2.b demonstrate that the performance of DPM and AES processing on the suggested platform (Figure 2.a) is identical to that of a single string (in Figure 2.b).

Quality characteristics, which include service standardization and independence, are another factor that can be assessed.

A client can access the platform by utilizing the offered generic service, as stated in Code I. Users can engage with cloud services without worrying about their requirements or the output type of a service since the service is independent of the cloud value-added services at the BTaaS. For

instance, in Scenario 1, a client-side application retrieves data without being aware of the database's kind or location. Any type of service at BTaaS may be bound to a service at FTaaS.

In Scenario I, many cloud vendors are able to specify comparable services at FTaaS, allowing an eHealth system to leverage various cloud standardized services.

V. CONCLUSION

Using a cloud SOA architecture called DCCSOA, we suggested a dynamic cloud platform for an eHealth system in this study. A cloud vendor can standardize and personalize services with the suggested platform running on top of heterogeneous cloud computing platforms with little to no modification The platform makes use of a template layer divided into two parts: FTaaS, which lets cloud vendors establish a standard, generic, and uniform service, and BTaaS, which lets defined services at BTaaS tie to the cloud vendor value-added services. In order to assess the performance of the suggested platform, we also developed a data access scenario on it using two distinct approaches. AES encryption is the second way, and the first is a simple data privacy method (DPM).The evaluation demonstrates the platform's scalability and the lack of additional overhead introduced by the methods used on the platform.

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] [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] [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 Rulebased 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