Asian Journal of Research in Computer Science

2(3): 1-15, 2018; Article no.AJRCOS.46069

Sharing of Patient Health Record (PHR) in Jelastic Cloud in a Secured Manner

Umme Afifa Jinan[1] and Sultana Jahan Soheli[1*]

[1]Department of Information and Communication Engineering, Noakhali Science and Technology University, Noakhali, Bangladesh.

Authors' contributions

This work was carried out in collaboration between both authors. Author UAJ designed the study, developed the model and did necessary research and system development. Author SJS managed the literature searches and wrote the first draft of the manuscript. Both authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJRCOS/2018/v2i328759
Editor(s):
(1) Dr. Young Lee, Associate Professor, Department of Electrical Engineering and Computer Science, Frank H. Dotterweich College of Engineering, Texas A&M University-Kingsville, USA.
(2) Dr. Sasikumar Gurumoorthy, Professor, Department of Computer Science and Systems Engineering, Sree Vidyanikethan Engineering College, India.
(3) Dr. Stephen Mugisha Akandwanaho, Senior Lecturer, Department of Information Systems and Technology, University of KwaZulu-Natal, South Africa.
Reviewers:
(1) Anthony (Tony) Spiteri Staines, University of Malta, Malta.
(2) Oyeleye, Christopher Akinwale, Ladoke Akintola University of Technology, Nigeria.
(3) Iroju Olaronke, Adeyemi College of Education, Nigeria.
(4) Anand Nayyar, Duy Tan University, Vietnam.
Complete Peer review History: http://www.sdiarticle3.com/review-history/46069

Original Research Article

Received 25 October 2018
Accepted 04 January 2019
Published 21 January 2019

ABSTRACT

Now-a-days cloud computing is a prominent way of providing resources and services in very secure manner. Gradually more and more organizations, companies and industries are picking up cloud technology for the safe keeping of their data. The objective of this work is to apply cloud service in healthcare system by building a practical patient health record (PHR) application and deploying it in the cloud. The system is 'doctor-centric' health record portal where only the doctor or hospital authority is responsible for securing their patients' health data and this labor-free, paperless system is giving relief to the doctors and hospital authorities from various error-prone traditional health record keeping systems. Jelastic cloud is used to provide cloud service to the developed application which provides security, scalability, quality of service and ease of maintenance of the application. Jelastic cloud also provides load balancing whenever the user load is high. We are developing an interactive PHR application which is dynamically storing, creating, modifying and maintaining data and deploying it in the Jelastic CloudJiffy server by the use of

**Corresponding author: E-mail: sohelisoha@gmail.com;*

InMotion Hosting server. CloudJiffy is India based fully redundant, high performance and scalable cloud "Platform-as-a-Service (PaaS)" under Jelastic Cloud Union. The whole system will be an efficient way for safe keeping Patients' health records, their medical history and sensitive health information in a pervasive, confidential manner. The system is highly compatible for preserving medical records of eminent persons of our society and for those whose health information must be kept confidential in a highly secure way.

Keywords: Patient Health Record; Jelastic Cloud; Cloud Jiffy Server; InMotion Server; PaaS.

1. INTRODUCTION

Cloud computing is a new way of delivering computing resources and services which provides functionality for managing information in a distributed and pervasive manner supporting several platforms, systems and applications [1]. Cloud computing is a subscription-based service where one can obtain networked storage space and computer resources [2]. It provides flexible and cost effective way to access the data to end users in multiplatform at any time [3]. There are different cloud deployment models namely Public Cloud, Private Cloud, Community Cloud and Hybrid Cloud. Existing processes for patients' vital data collection require a great deal of labor work to collect, input and analyze the information which are usually slow and error prone [4]. The digitally managed **EHR** (Electronic Health Records)/**PHR** (Patient Health Records) systems in cloud based services offer advantages like cost reduction, data security, redundancy, privacy and availability [5]. The integration of healthcare with the Internet and smart technologies has led to increased accessibility to healthcare providers, more efficient processes and higher quality of healthcare services [6]. With the advancement of Information Technology, current healthcare systems are being transformed from traditional scenario that requires manual care and monitoring to more advanced scenario where patients can be automatically monitored [7]. The 21st century Healthcare Information Technology (HIT) has created the ability to electronically store, maintains, and move data across the world in a matter of seconds and has the potential to provide healthcare with tremendous increasing productivity and quality of services. It permits each provider to have his own database of Electronic Medical Records. The cloud computing market in the health care sector is expected to grow by 2017 to $5.4 billion. Hence from this survey [8] it can be interpreted that the applications of cloud in healthcare is going to be a huge industry in the near future [9]. Cloud computing based healthcare system makes it quite easy to get healthcare services over the internet using a web browser on a range of devices. Cloud data storage and maintenance frameworks offer a cost effective solution to the problem with increased security and ease of management. Patient records can be stored in Jelastic cloud in order to maintain a secure environment for digitally maintained PHR application. Jelastic cloud is a cloud service provider for hosting providers, telecommunication companies, enterprise and developers [10]. It is a new type of cloud hosting provider which combines PaaS(platform as a service) and CaaS(Container as a service) which supports languages such as Java, PHP, Ruby, Node.js, Python, .NET. We can buy servers, configure our OS, configure application server, and configure database and then start deploying our code all at a time simply by hosting Jelastic cloud. It is easy to start, deploy, scale, manage and load balancing is high which supports up to 12 cloudlets [11]. It supports 'Pay as You Use' service unlike other cloud services.

The work is carried out in order to Establish a secure platform for maintaining EHR/PHR application in clouds, study the feasibility of this platform for building practical patient record management system in hospitals and health organization in Bangladesh within limited resources and deploying the PHR application in Jelastic cloud for secure, scalable and ease of maintenance of the application.

The main objective of this work is to:

i. Meet the challenge of enhancing efficiency and quality of healthcare. Measures and outcome of procedures for diagnosis and therapy must be documented, communicated and evaluated carefully.
ii. Establish a secure platform for maintaining EHR (Electronic Health Records)/ PHR (Patient Health Records) application in jelastic cloud.
iii. Study the feasibility of this platform for building practical patient record

management system in hospitals and health organization in Bangladesh within limited resources.

iv. Deploy the PHR application in Jelastic cloud for secure, scalable and ease of maintenance of the application.

2. RELATED WORKS

Ming L et al., 2013 developed a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers to achieve fine grained and scalable data access control for PHRs, they proposed attribute based encryption (ABE) techniques to encrypt each patient's PHR file [12]. In this work, they considered the server to be semi-trusted, honest but curious. To achieve "*patient-centric*" PHR sharing, a core requirement is that each patient can control who are authorized to access to her own PHR documents. Especially, user controlled read/write access and revocation are the two core security objectives for any electronic health record system. The key idea is to divide the system into multiple security domains (namely, *public domains* (PUDs) and *personal domains* (PSDs)) according to the different users' data access requirements. In both types of security domains, they utilized ABE to realize cryptographically enforced, patient-centric PHR access.

Mangla N et al., (2014) illustrated that cloud computing has emerged as one of the enabling technologies that allows the business and IT world to use computer resource effectively and efficiently [13]. The main objective of this work is to outline the steps involved in developing and deploying applications for Microsoft Azure Cloud Platform. It also includes the performance analysis of cloud hosting over traditional web hosting. The sample application is a website, designed using the Microsoft Visual Studio environment and utilizing open source .NET templates; in order to illustrate the services and features associated with Microsoft Azure Platform.

Maheswari S and Upendra G (2017) developed a system where they showed that secure sharing of patient health records in Jelastic cloud provides the more benefits to the data owners and end users. In this paper [14], they propose an Attribute based encryption (ABE) algorithm for encryption and decryption of patient health records. This algorithm is encrypting the data before storing the PHR information to the cloud server. And decrypt the data while retrieving from server based on the attribute and access policy given by Data owner. Building a specialized data center's is very difficult task and maintenance cost also very high. Sharing the PHR Application in the third party server raises the security and privacy risks. Not only this, for providing the Scalability, Load balancing and for easy maintenance to the application, they deployed the Personal health record's application into Jelastic cloud by the use of Servant server.

Khandelwal P & Sharma R (2013) designed and implemented FADE, a secure overlay cloud storage system which is able to achieve fine-grained, policy-based access control and file assured deletion. It associates the outsourced files with file access policies, and assuredly deletes files to make them unrecoverable by anyone upon revocations of file access policies [15]. For achieving such security goals, FADE is built upon a set of cryptographic key operations that are self-maintained by a quorum of key managers that are independent of third-party clouds. Particularly, FADE acts as an overlay system which works seamlessly atop today's cloud storage services. They implemented a proof-of-concept prototype of FADE Jelastic, one of today's cloud storage services. They conducted extensive empirical studies, and demonstrated that FADE provides security protection for outsourced data, while introducing only minimal performance and monetary cost overhead.

Subhasri P and Padampriya A [16] showed some important issues and proposed that the evolution of cloud computing in healthcare management systems provides better storage and sharing of medical records through the network. In healthcare systems, cloud not only facilitates the exchange of electronic medical records but it also enables to share the contents in a secured way. The storage of HIS (Healthcare Information Systems) in cloud provides greater flexibility but at the same time it has security issues. In this paper the various challenges involved in sharing healthcare information through cloud platform is described. The issue associated with sharing of information especially medical images through cloud, the existing solutions and its limitations are also discussed in this work.

Trieu C et al. [17] proposed a model where they showed that scalability as a critical issue to the success of many enterprises currently involved in doing business on the web and in providing information that may vary drastically from one time to another. Maintaining sufficient resources just to meet peak requirements can be costly. Cloud computing provides a powerful computing model that allows users to access resources on- demand. In this paper, they described an architecture for the dynamic scaling of web applications based on thresholds in a virtualized Cloud Computing environment. A dynamic scaling algorithm for automated provisioning of virtual machine resources based on threshold number of active sessions will be introduced. The on-demand capability of the Cloud to rapidly provision and dynamically allocate resources to users will be discussed. Our work has demonstrated the compelling benefits of the Cloud which is capable of handling sudden load surges, delivering IT resources on-demands to users, and maintaining higher resource utilization, thus reducing infrastructure and management costs.

Carlos O et al. [18] proposed that existing processes for patients' vital data collection require a great deal of labor work to collect, input and analyze the information. These processes are usually slow and error prone, introducing a latency that prevents real-time data accessibility. This scenario restrains the clinical diagnostics and monitoring capabilities. They proposed a solution to automate this process by using “sensors” attached to existing medical equipment that are inter-connected to exchange service. The proposal is based on the concepts of utility computing and wireless sensor networks. The information becomes available in the “cloud” from where it can be processed by expert systems and/or distributed to medical staff. The proof-of-concept design applies commodity computing integrated to legacy medical devices, ensuring cost effectiveness and simple integration.

Lakshmi P [19] discussed the healthcare services available in the new converging technology called cloud computing. This computing technology had craved its path in the desirable market field healthcare. This study represented an overview of the healthcare transformation of different approaches of cloud computing over information technology and its strategic usage. Further enhancing better healthcare to ensure scalable, compatible functions supporting the well-being, this study also considers the techniques of cloud computing and its application, advancement in healthcare.

Talal H et al. [20] explained that trust is one of the most concerned obstacles for the adoption and growth of cloud computing. Although several solutions have been proposed recently in managing trust feedbacks in cloud environments, how to determine the credibility of trust feedbacks is mostly neglected. In this paper, they proposed a framework that uses web services to improve ways on trust management in cloud environments. In particular, they introduced an adaptive credibility model that distinguishes between credible and malicious feedbacks by considering the cloud service consumer’s capability and majority consensus of their feedbacks. They also presented a replication determination model that dynamically decides the optimal replica number of the trust management service so that the trust management service can be always maintained at a desired availability level. The approaches have been validated by a prototype system and experimental results.

Charalampos D et al. [21] proposed a system prototype, where they discussed that cloud computing provides functionality for managing information data in a distributed, ubiquitous and pervasive manner supporting several platforms, systems and applications. This work presents the implementation of a mobile system that enables electronic healthcare data storage, update and retrieval using Cloud Computing. The mobile application is developed using Google’s Android operating system and provides management of patient health records and medical images (supporting DICOM format and JPEG2000 coding). The developed system has been evaluated using the Amazon’s S3 cloud service. This article summarizes the implementation details and presents initial results of the system in practice.

Sekhar T et al. [22] stated an argument that deploying state-of-the-art technologies is vital and inevitable in assistive healthcare to cope with emerging services such as remote monitoring, collaborative consultation, and electronic health record. This work proposes Mobile Cloud for Assistive Healthcare (MoCAsH) as an infrastructure for assistive healthcare. Besides inheriting the advantages of Cloud computing, MoCAsH embraces important concepts of

mobile sensing, active sensor records, and collaborative planning by deploying intelligent mobile agents, context-aware middleware, and collaborative protocol for efficient resource sharing and planning. MoCAsH addresses security and privacy issues by deploying selective and federated P2P Cloud to protect data, preserve data ownership and strengthen aspects of security. It also addresses various quality-of-service issues concerning critical responses and energy consumption.

Nkosi M et al. [23] explained that Mobile devices are being considered as service platforms for mobile health information delivery, access and communication. However mobiles face challenges with regard to delivering secure multimedia based health services due to limitations in computation and power supply. Since mobile devices have limited computational capacity and run on small batteries; they are unable to run heavy multimedia & security algorithms. In this paper a cloud computing framework to relieve mobile devices from executing heavier multimedia and security algorithms in delivering mobile health services is described. The proposed framework uses a Cloud Computing protocol management model which intends to provide multimedia sensor signal processing & security as a service to mobile devices. Our approach suggests that multimedia and security operations can be performed in the cloud, allowing mobile health service providers to subscribe and extend the capabilities of their mobile health applications beyond the existing mobile device limitations.

Alshammari A et al. [7] discussed many important and latest issues in cloud computing and showed that Cloud Computing has emerged as a new paradigm of computing that builds on the foundations of Distributed Computing, Grid Computing, and Virtualization. Cloud computing is Internet-accessible business model with flexible resource allocation on demand, and computing on a pay-per-use as utilities. Cloud computing has grown to provide a promising business concept for computing infrastructure, where concerns are beginning to grow about how safe an environment is. Security is one of the major issues in the cloud-computing environment. In this paper we investigate some prime security attacks and possible solutions for clouds: XML Signature Wrapping attacks, Browser Security, and Vendor Lock-in.

Benaloh J et al. [3] explored the challenge of preserving patients' privacy in electronic health record systems. They proposed that security in such systems should be enforced via encryption as well as access control. Furthermore, they stated approaches that enable patients to generate and store encryption keys, so that the patients' privacy is protected should the host data center be compromised. The standard argument against such an approach is that encryption would interfere with the functionality of the system. However, they showed that they can build an efficient system that allows patients both to share partial access rights with others, and to perform searches over their records. They formalized the requirements of a Patient Con- trolled Encryption scheme, and give several instantiations, based on existing cryptographic primitives and protocols, each achieving a different set of properties.

3. METHODOLOGY

The proposed model concentrates on providing Security, Privacy, Scalability, Load balancing, and Easy maintenance to the personal health records application in the cloud. The elaboration of the system and its design and architecture, illustration of tools and materials required to implement the system and the working procedure of each modules comprising the system are discussed in detail. To improve the overall conventional medical record system, we have designed an interactive, labor-free, paper-less digitally maintained patient health record (PHR) system which will provide benefits to both doctors and patients to a greater extent.

3.1 Design

The proposed patient health record application comprises of this two fields: Authority/Admin & Doctor (Or Hospital Authority). In this system, first we have kept the registration process to access the PHR system. The user/doctor will register from the given signup option. Thus they will be able to access the PHR system. After accessing to the system, doctors or users can dynamically create, read, update and delete their own patients' health records which they have created. They can check patients' medical history and all other information patients have provided to them. Following this, they can observe patients overall condition and give treatment accordingly [24]. All the information will be reserved in the patients'

database and thus there is no possibility of losing medical records or having wrong, irrelevant information in the patient database. Fig. 1 below gives an overview of the system.

I) Workflow Diagram

The total system will give relief to the patients from keeping prescription papers or fear of losing them. The PHR system will be highly secure. If there is Internet connection in the target area, any hospital authority or doctor can access the PHR system from anywhere and be benefitted. Fig. 2 depicts Work Flow Diagram of the PHR System. From the structure of Work Flow Diagram of the PHR System, it is seen that user will first login or signs up to the admin panel through providing their username and password and fill up other fields necessary to access the system. After login or signup, they will access the system. They will perform CRUD (create, read, update, delete) operation on the database. Any modification of data will be dynamically stored in the database. Each user will maintain and be responsible for his own database record. Thus, the PHR system will be doctor-centric and highly as patients don't have to provide health information on their own and only the doctors or hospital authority will store patients' information.

3.2 Deployment in Jelastic Cloud

After we have developed the interactive Patient Health Record (PHR) application, we would perform necessary steps to deploy it in the Jelastic cloud server. Jelastic cloud provides us with high security, scalability and easy maintenance to the PHR application in cloud. Jelastic Cloud also provides the Load balancer to our application. It can easily scale horizontally and vertically in the both ways whenever user load is high [19]. In order to deploy the PHR application in the Jelastic cloud, first we need to create appropriate environment for deploying it. We will use InMotion hosting server to create such environment. We will also use Nginx as our web server. As seen from figure two, the users are marked as either doctors or any hospital authority. They can access the system, view and update their patients' records. As we discussed before, the whole system is highly secure. The PHR owner maintains the system, performs any tasks necessary to update the system. The owner will deploy the system in the Jelastic cloud [16]. First, the owner will manage the application in order to make it compatible for deployment with the help of InMotion Hosting Server and then deploy it in the cloud. Jelastic cloud will provide high security, vertical and horizontal scalability, load balancing to our PHR application. Next figure will show Architecture of PHR Application in Jelastic Cloud. Where two types of users (doctor and/or hospital authority) can log on the PHR system by using their credentials (user id, password, etc.) and it's a two way communication-authentication process. For authenticating the users, PHR system will verify the data with the stored data in InMotion hosting server. Then the users can upload their necessary data. After completing the data if all the information are correct and verified to be authentic then the data will be stored in the jelastic cloud and when user want to download/use the data they have to log on the system and download it.

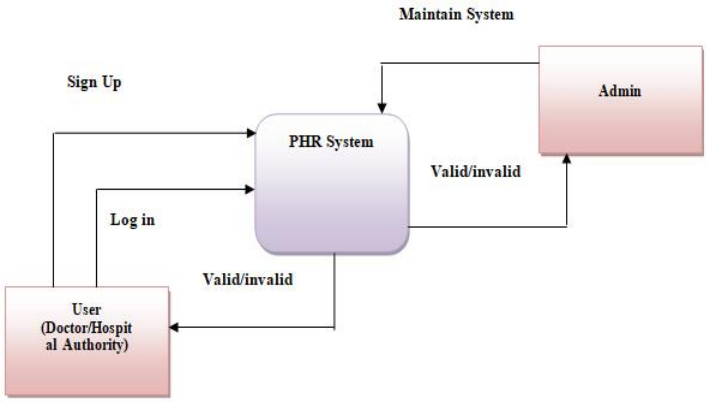

Fig. 1. Overall Structure of the PHR system

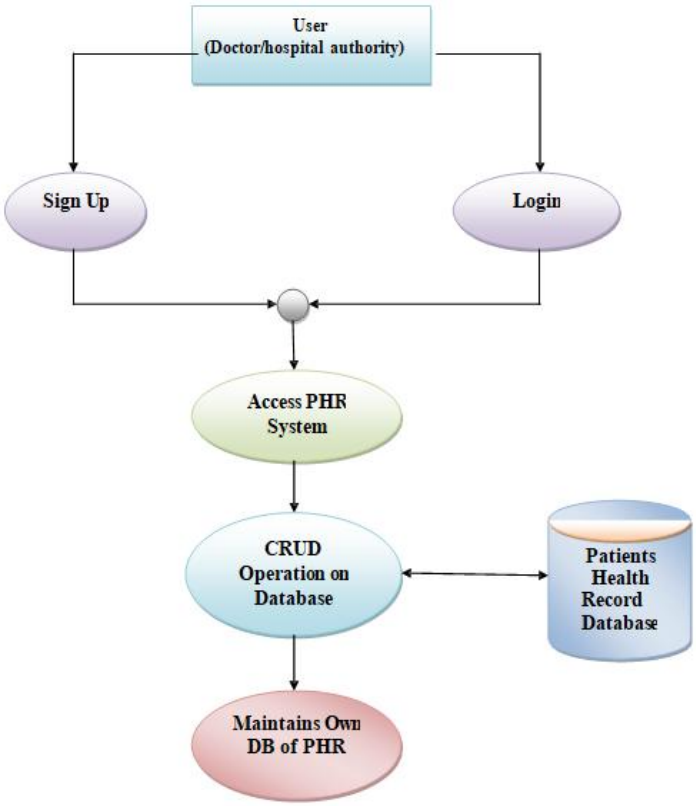

Fig. 2. Work Flow Diagram of the PHR System

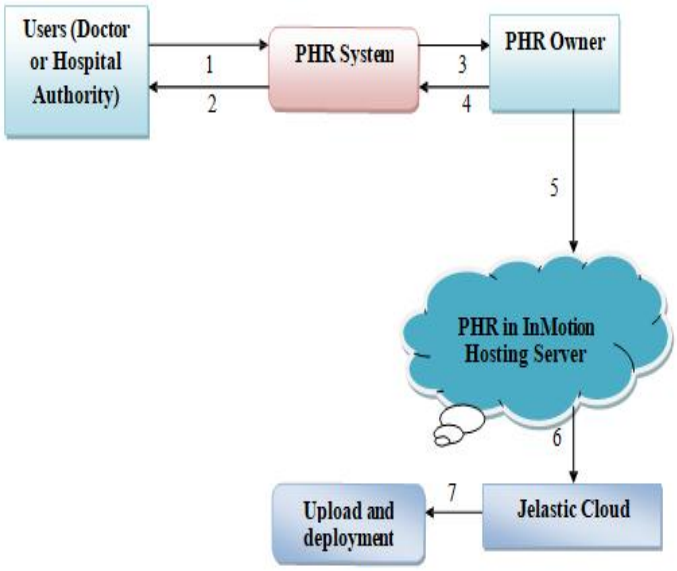

Fig. 3. Architecture of PHR system

Next figure will show Jelastic Application deployment method. There are four methods for deploying files in Jelastic Cloud. Among these four method second method is used for our work.

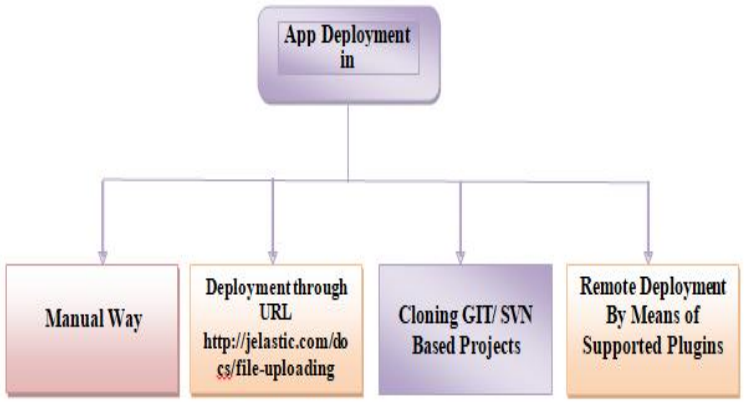

Fig. 4. Jelastic Application Deployment Methods.

4. IMPLEMENTATION AND ANALYSIS

In this part implementation technique and the developed system is analyzed with necessary screenshots. As it's a pretty big system some screenshots are skipped. Following Fig. 5 show the Login Page. For log in user have to insert there credentials like user name and password. But if the user is new then he/ she have to create account first.

After logging in or signing up, we get the index page like Fig. 6 (b). The index page provides an overview of the PHR application and users can start their work from it. They can go through patients' database, get a new form for storing a new patient's record and again come back to the index page simply by accessing the side bar provided in the page.

They can also be logged out from the application by clicking the option 'Log Out' given in the top right corner. By accessing this page, user can add a new record of patients' personal and health information (as Fig. 7). They can create as much new records as they want. Some mandatory information are marked here which must be provided by the patients. After all the information has been provided by the patient, the record will be dynamically stored to the database.

The page (as Fig. 8) shows the database of the patients that the users have created and stored. This database is dynamic, users can update, delete any information from this database. When users create a new patient record, the record will be dynamically added to the database. There is also a search bar on top of the patients list and users can search by name, ID or number for a quick search to the database and find a specific patient.

I) Update Patient Health Record Page

Users can select any health record list from the database of the patients' list and update existing information that patients have provided earlier. After any modification of the health information, the updated record will be restored to the patients' database of health records.

II) Deployment Processes in Jelastic Cloud

After developing the PHR application, we would proceed to deploy it in the Jelastic cloud. We have created appropriate environment with the help of InMotion Server to deploy our PHR application. First, we have selected the "CloudJiffy" Jelastic service provider for deployment. CloudJiffy is India based fully redundant, high performance and scalable cloud "Platform-as-a-Service (PaaS)" under Jelastic Cloud Union which is a multi-cloud PaaS for developers which can be downloaded from the site

(https://cloudJiffy.com) [25]

The following screenshots provides an overview of the implementation process that was performed step by step in order to deploy the PHR application in the Jelastic CloudJiffy server:

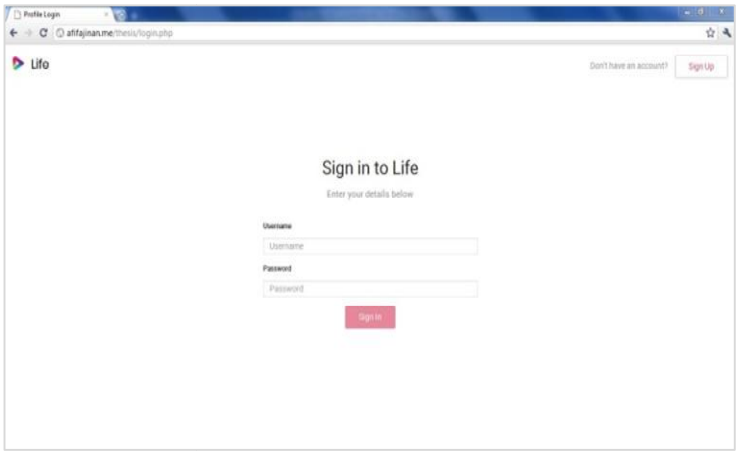

Fig. 5. The Login Page

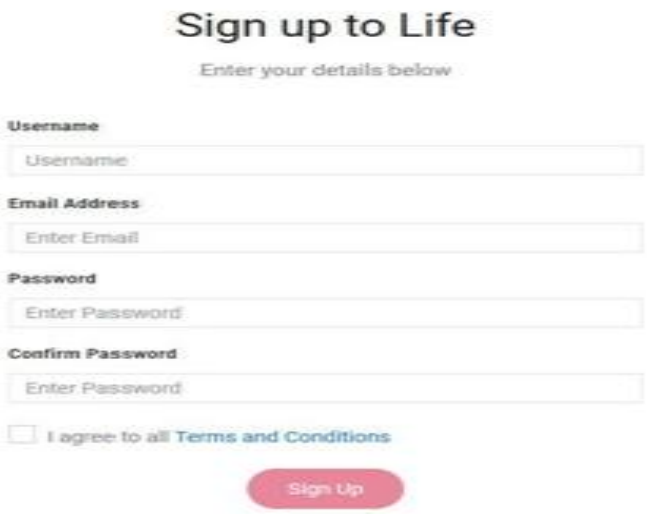

Fig. 6(a). Sign up Page

Fig. 6(b). Index Page

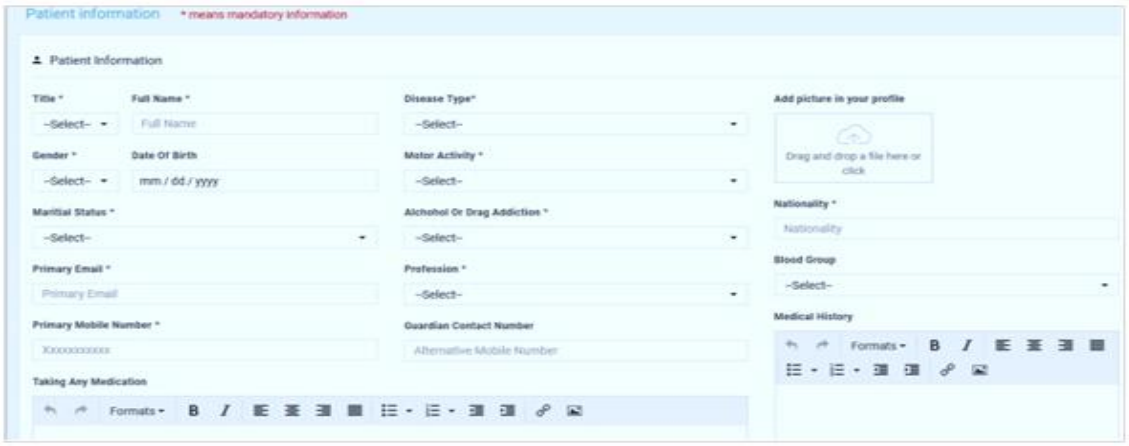

Fig. 7. Add New Patient Record Page

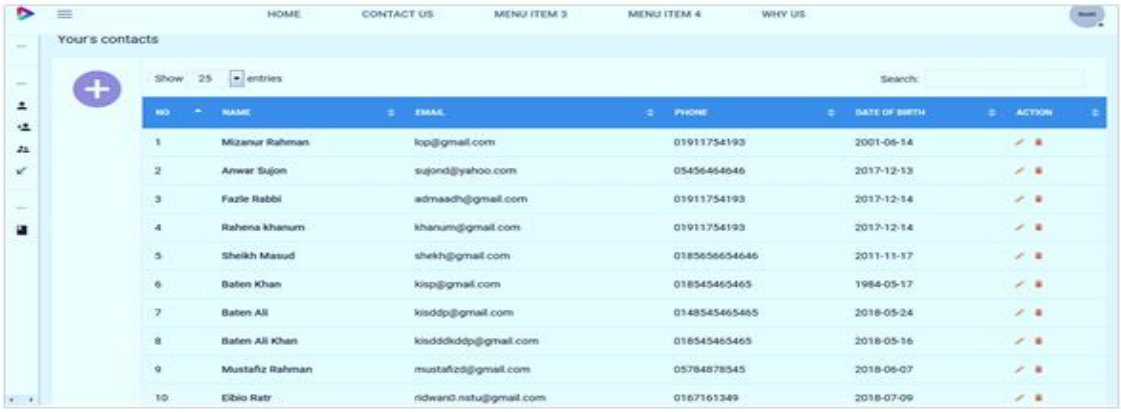

Fig. 8. Patient Health Record Database Page

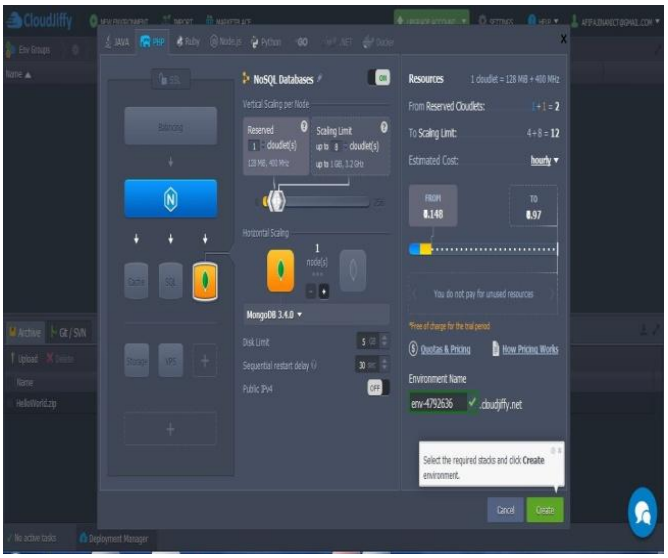

Fig. 9. Jelastic CloudJiffy User Dashboard

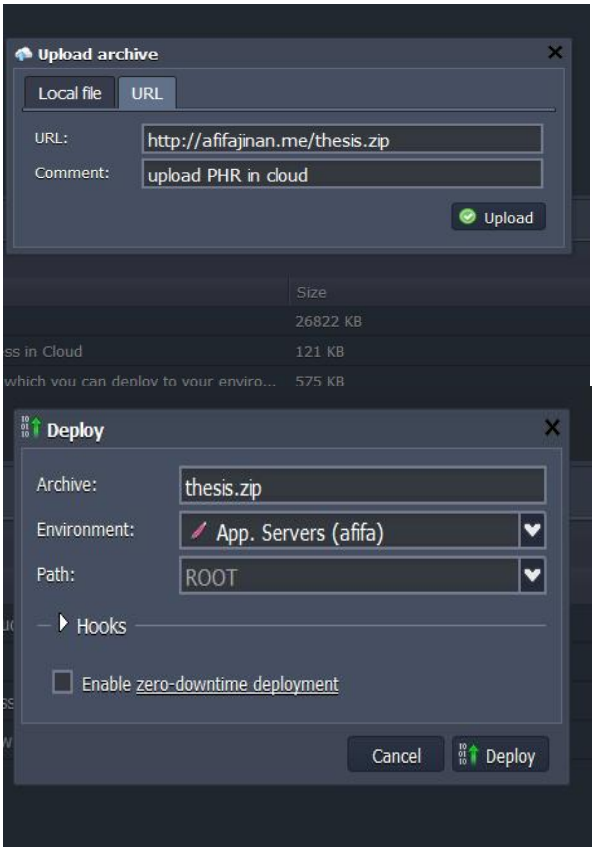

Fig. 10. Uploading & Deploying PHR application in Jelastic CloudJiffy

After signing up to the system, we have the user dashboard area to perform our tasks as shown in the figure above. In the dashboard area, we have to select PHP environment, Apache server, vertical and horizontal scaling as per our needs, choose as many cloudlets as required up to twelve. We give an environment name and finally create an environment in the cloud. Then we have to create Environment for Deploying PHR Application. After we have selected necessary installations and server requirements to create an environment in the cloud server, we get an overview as shown in the figure above which shows us that an environment named afifa has been created in the cloud server. A notification named 'Running' also shows us that this environment is currently running among several others.

III) Application Upload

The following screenshot comes up with the uploading process of or PHR file in the cloud. First we have to upload the PHR file in the cloud in zipped format in order to deploy it later. We have selected the URL and drop the link and leave a comment [26].

We have successfully deployed our PHR application in the Jelastic CloudJiffy server. We have exported the PHR database from the hosting server to the cloud environment and make some necessary changes in the cloud and finally deployed it in the cloud. Our application is working fine in the CloudJiffy server. The deployed PHR application will be highly secure, scalable and load balancing will also be maintained in this server.

We can access the application from the link given below:

For registered user:

node6314-afifa.cloudjiffy.net/project/login.php

For unregistered user:

node6314-afifa.cloudjiffy.net/project/signup.php

IV) Security Implementation

As our system is developed as a prototype here some common and easily available security measures are used [27,28]. All data of the system are sent as zip files and encrypted with a password. To accomplish this password purpose B1 Free Archiver a free multiplatform compression tool is used. For creating the archive just need to check the "Protect with a password" option from the menu, type in the password and only after that the zipped and secured file can be moved to the cloud [29]. Then for some cases the password can be shared with the admin. Note that B1 Free Archiver zips files only in B1 format which makes the overall protection of patient health record more reliable. The only software that opens B1 files is B1 Free Archiver, therefore it is not possible to open any B1 archive, even one that isn't password-protected, without this utility. B1 encrypted archives appear to be safer and secure than the usual zip files. Beside password protection a higher level protection for all sensitive information of the system, an open source encryption software TrueCrypt is used [30]. This software creates encrypted file of system information that needed to be kept in the cloud like virtual disk and protected with password. In TrueCrypt AES algorithm is used for encrypting the information. But it is also possible to use Serpent, Twofish etc. for the encryption purpose. As Jelastic Multi-Cloud DevOps PaaS has a built in security measure Shield 5.4, within this release, the platform was upgraded with a new firewall management system, private network isolation and a set of other features demanded by customers. This shield can manage inbound and outbound firewall rules on the container level through a convenient graphical interface. A number of default rules are automatically added to the inbound section to make the node operable. As shown in Fig. 11, whenever the data from cloud is used the firewall state will be on for security insurance. All the inbound connections are denied by default according to jelastic cloud traffic rules, so that the data stored in the cloud cannot be captured by someone else rather than intended user. And “inbound traffic rules” are set before the system operation. And in case of outbound connections by default all are allowed except those are not allowed according to the rules set (Fig. 11). Also, automatic network isolation is implemented to prohibit any unallowed connections between different environments. This results in another essential newly added possibility to create secure environment groups, intended to isolate environments of a single account from each other. Platform automatically creates a dedicated IP set for each isolated group, which is composed of the appropriate containers internal addresses. This allows controlling access between nodes of each environment. In Fig. 12 the group creation is shown. Where some credentials name, parent group and environment must be put and network isolation must be on.

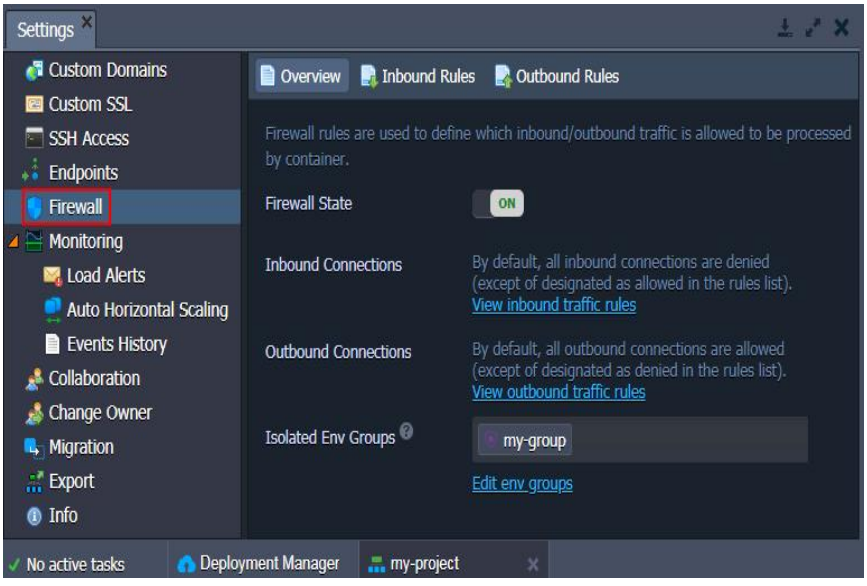

Fig. 11. Option of inbound and outbound firewall rules

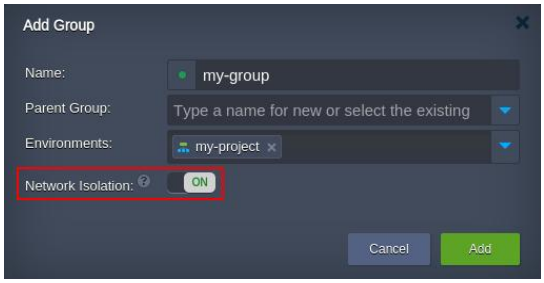

Fig. 12. Option for create secure group in jelastic cloud

In confines of Jelastic Shield version, there were added a number of other demanded features and improvements, among them [31]:

- Extra Environment Layers for All Supported Middleware Stacks.
- Go Language Support via a Specially Packaged Middleware Container.
- Webhooks for Application Build and Deploy Operations.
- Built-In Web SSH Console.
- HTTP 2.0 Support for Jelastic Shared and Dedicated Load Balancers.
- UI/UX Improvements.
- Deployment Improvements.
- Cloud Scripting Engine Optimization for Improved Serverless User Experience.

And in future other high level security algorithms will be implemented for more secure sharing of the patient health record and other information [32].

5. CONCLUSION AND FUTURE SCOPE

This work focuses on secure sharing of patient health records in Jelastic cloud. We have developed an interactive, efficient PHR scheme which is dynamic, highly secure and user-friendly. Multiple doctors or hospital authorities can access the system and have personal accounts where they will store their own patients' health information. As the doctor or the hospital authority is the only responsible person or entity for preserving patients' health information, there is no chance of providing any wrong information and the records are highly secure and kept confidential. The patients often provide wrong information when they are chosen to provide on their own. Patient health record security is crucial especially for the prominent figures of the country or society such as politicians, social figures, eminent persons who play a major role in society and country governance. Any exposure of impressionable past history revolving medical records can create an unrest situation in the society. Preserving medical records of criminals is also important in crime investigation, National Defense and Intelligence departments. So, the application that we have created will preserve patients' health records in a highly secure way and thus the society will be benefitted.

6. FUTURE SCOPE

The proposed system works on developing an efficient patient health record scheme that provides easy, labor-free record of patient health data electronically. It will serve as an effective way for recording patients' health history, current records and thus will lessen doctors' effort to a greater extent. PHR security is a major issue in developed countries and soon it will emerge in Bangladesh too. Currently we are working on developing a security scheme to preserve and maintain patient health record using secure algorithm like Attribute Based Encryption (ABE) [33] and Truecrypt/ BitLocker finally deploy it on Jelastic cloud. ABE is a highly secure algorithm for encrypting data and we wish to apply it to our PHR information before outsourcing it to the cloud in near future.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Mell P, Grance T. The NIST definition of cloud computing; 2011.
Available:https://dl.acm.org/citation.cfm?id=2206223
(Accessed on 02.02.2018)
2. Huth A, Cebula J. The basics of cloud computing.
Available:https://www.us-cert.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf
(Accessed on 25.01.2018)
3. Benaloh J, Chase M, Horvitz E, Lauter K. Patient controlled encryption: Ensuring privacy of electronic medical records. Proceedings of the 2009 ACM workshop on Cloud computing security. 2009;103-114.

Available:http://www.enggjournals.com/ijet/docs/IJET17-09-05-324.pdf
(Accessed on 13.11.2017)

4. Adrian B. Java hosting platform jelastic adds NGINX. Dr. Dobb's Journal. Archived from the original; 2015.
Available:http://www.drdobbs.com/opensource/javahostingplatform-jelastic-adds-ngin/231901927
(Accessed on 14.11.2017)
5. Alejandre F. Secure exchange of information in electronic health records.
Available:https://ro.uow.edu.au/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=4308&context=these
(Accessed on 01.01.2018)
6. Shuo L, Yuan H, Qian L, Lingyu W, Rachida D. Implementing web-based e-health portal systems.
Available:https://www.albany.edu/faculty/hong/pub/eHealthPortal.pdf
(Accessed on 01.01.2018)
7. Alshammari A, Alhaidari S, Alharbi A, Zohdy M. Security threats and challenges in cloud computing. 4th International Conference on Cyber Security and Cloud Computing (CSCloud). 2017;46-51. IEEE.
Available:https://ieeexplore.ieee.org/document/7987175
(Accessed on 10.12.2017)
8. Available:https://electronichealthreporter.com/healthcare-will-invest-5-4-billion-in-cloud-computing-by-2017/
(Accessed on 28.02.2018)
9. Bangladesh Health Facility Survey. National Institute of Population Research and Training (NIPORT), Ministry of Health and Family Welfare, "AWS vs. Azure vs. Jelastic in Wordpress Development"; 2014.
Available:https://blogi.datacenter.fi
(Accessed on 18.12.2017)
10. Khandelwal P, Sharma R. Cloud access security on file system using secure policies for jelastic cloud. International Journal of Computer Applications in Engineering Sciences. 2013;3(4):136.
(Accessed on 26.01.2018)
11. Rolim O, Koch L, Westphall B, Werner J, Fracalossi A, Salvador S. A cloud computing solution for patient's data collection in health care institutions. In eHealth, Telemedicine, and Social Medicine, ETELEMED'10. Second International Conference. IEEE. 2010;95-99.
Available:https://ieeexplore.ieee.org/document/5432853
(Accessed on 02.02.2018)
12. Ming L, Shucheng Y, Yao Z, Kui R, Wenjing L. Scalable and secure sharing of personal health records in cloud computing using attribute-based Encryption. IEEE Transactions on Parallel and Distributed Systems.
Available:https://ieeexplore.ieee.org/abstract/document/6171175
(Accessed on 10.02.2018)
13. Mangla N, Singh J, Singh M. Improving performance of web applications using cloud resources. In Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 2014 3rd International Conference. IEEE. 2014;1-6.
Available:https://ieeexplore.ieee.org/document/7014765
(Accessed on 06.02.2018)
14. Maheswari S, Gudla U. Secure sharing of personal health records in Jelastic cloud by attribute based encryption. In Advanced Computing and Communication Systems (ICACCS). 4th International Conference on IEEE. 2017;1-4.
(Accessed on 07.02.2018)
15. Khandelwal P, Sharma R. Cloud access security on file system using secure policies for jelastic cloud. International Journal of Computer Applications in Engineering Sciences. 2013;3(4):136.
(Accessed on 10.02.2018)
16. Subhasri P, Padampriya A. A security issues involved in sharing of healthcare information's through cloud storage.
Available:http://www.enggjournals.com/ijet/docs/IJET17-09-05-324.pdf, ISSN (Print): 2319-8613
(Accessed on 13.01.2018)
17. Trieu C, Ajay M, Alexei A, Alla S. Dynamic Scaling of Web Applications in a Virtualized Cloud Computing Environment.
Available:https://ieeexplore.ieee.org/document/5342101
(Accessed on 12.02.2018)
18. Carlos R, Fernando K, Carlos W, Jorge W, Armando F, Giovanni S. A cloud computing solution for patient's data collection in Health Care Institutions. Second International Conference on eHealth, Telemedicine, and Social Medicine; 2010.

Available:https://ieeexplore.ieee.org/document/5432853
(Accessed on 28.12.2017)
19. Kuchimanchi P. Healthcare Services In Cloud Computing; 2016.
Available:https://www.researchgate.net/publication/309088652_
(Accessed on 09.01.2018)
20. Noor H, Sheng Z. Web service-based trust management in cloud environments. In Advanced Web Services. Springer, New York, NY. 2014;101-120.
Available:https://link.Springer .com/
Chapter /10.1007/978-1-4614-7535-4_5
(Accessed on 05.02.2018)
21. Charalampos D, Thomas P, Ilias M. Mobile healthcare information management utilizing Cloud Computing and Android OS.
Available:https://ieeexplore.ieee.org/document/5628061
(Accessed on 12.02.2018)
22. Sekhar S, Kumar K. Mobile Cloud for Aiding and Hard- wearing Healthcare; 2010.
Available:https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3892841/
(Accessed on 31.01.2018)
23. Nkosi M, Mekuria F. Cloud computing for enhanced mobile health applications. IEEE Second International Conference on Cloud Computing Technology and Science; 2010.
Available:https://ieeexplore.ieee.org/document/5708511
(Accessed on 09.02.2018)
24. Huang C, Yan K, Wei S, Zhang G, Lee H. Efficient anonymous attribute -based encryption with access policy hidden for cloud computing. In Progress in Informatics & Computing (PIC). December International Conference on IEEE. 2017; 266-270.
Available:https://ieeexplore.ieee.org/document/8359555
(Accessed on 05.01.2018)
25. Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In International Workshop on Public Key Cryptography. 2011;53-70.
Available:https://eprint.iacr.org/2008/290.pdf. Springer, Berlin, Heidelberg
(Accessed on 18.01.2018)
26. Multi cloud Pass for developers.
Available:https://jelastic.cloud/
(Accessed on 19.01.2018)
27. Mazhar A, Samee K, Athanasios V. Security in cloud computing: Opportunities and challenges.
Available:https://www.sciencedirect.com/science/article/pii/S0020025515000638
(Accessed on 09.02.2018)
28. Tips to keep your data secure on the cloud.
Available:https://www.cio.com/article/2380182/cloud-security/5-tips-to-keep-your-data-secure-on-the-cloud.html
(Accessed on 12.02.2018)
29. Study of b1.
Available:https://b1.org/
(Accessed on 19.02.2018)
30. TrueCrypt, Migrating from TrueCrypt to BitLocker.
Available:http://truecrypt.sourceforge.net/
(Accessed on 18.02.2018)
31. Available:https://jelastic.com/blog/cloud-protection -with-firewall-management-and-private-network-isolation-shield-54/
(Accessed on 28.02.2018)
32. Li M, Yu S, Zheng Y, Ren K, Lou W. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Transactions on Parallel and Distributed Systems. 2013;24(1):131-143.
(Accessed on 09.02.2018)
33. Zavattoni E, Perez D, Mitsunari S, Sánchez-Ramírez H, Teruya T, Rodríguez F. Software implementation of an attribute-based encryption scheme. IEEE Transactions on Computers. 2015;64(5): 1429-1441.
Available:https://ieeexplore.ieee.org/document/6827966
(Accessed on 22.01.2018)

Peer-review history:
The peer review history for this paper can be accessed here:
http://www.sdiarticle3.com/review-history/46069