EXPERIMENTAL STUDY ON SECURE AND AUDITABLE PERSONAL HEALTH RECORES OVER CLOUD STORAGE

ANANDA RAO M
Research Scholar, OPJS University,
Rajasthan.

Dr. VIJAYPAL REDDY
Associate Professor, Department of CSE
OPJS University, Rajasthan

ABSTRACT:

Now a day's increasing popularity of public cloud many personal health record (PHR) owners are outsourcing their sensitive documents to cloud but due to public and global access of cloud the PHR owner need to provide efficient security. Generally PHR system has multiple PHR owners and PHR users. The owners refer to patients who have full control over their own PHR data, i.e., they can create, manage and delete it. There is a central server belonging to the PHR service provider that stores all the owners" PHRs. The users may come from various aspects; like, a friend, a caregiver or a researcher. Users access the PHR documents through the server in order to read or write to someone's PHR, and a user can simultaneously have access to multiple owners" data. Correctness of the PHI in the cloud is put at risk due to the following reasons. Although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they still face a broad range of both internal and external threats to data integrity.

Keywords*: Cloud computing, Data privacy, Fine grained access control, Attribute based encryption (ABE).*

I. INTRODUCTION

Internet-based, on-demand computing where shared resources, data, information and other devices are available to user on-demand is known as Cloud Computing. The computing resources from shared pool are accessed by users on the basis of demand and store their data in third-party data centers at distant locations. At the establishment of cloud platform infrastructure and resources are the wider concept to achieve coherence and economies of scale. A model of cloud computing can be quickly adapted provisioned and quashed with least effort for enabling omnipresent, suitable, on demand network based access to a shared pool of configurable computing resources. To improve the effectiveness of the cloud resources are dynamically reallocated as per demand and shared by multiple users. With enhanced manageability and less maintenance cloud computing allows enterprises to acquire their applications up and consecutively more rapidly without purchasing licenses for different applications, Cloud computing ensures the access to single server by multiple users for retrieval and update of their data from cloud computing. Under the pay-as-you-go model (customers pay for services on pay-per-use basis) Cloud computing delivers infrastructure, platform, and software (applications) as subscription based services, which are provided to customers and supports hosting of pervasive applications from domestic, research and enterprise domains.

Cloud computing is recent development and has its roots in Grid Computing, or initial form of Parallel & Distributed Computing. Grid computing was modeled as volunteer ensemble of computing, storage and data resources. Respectively, such collaborative computing was named as computing grid, storage grid and data grid. As an electrical grid provides power and client pays back for the power drawn from grids, so was with grid computing framework. Clients may access grids for the services offered by grid and adopts

pay-as-you-use model. Grids computing also named utility computing as otherwise, unused resources are converted into a utility.

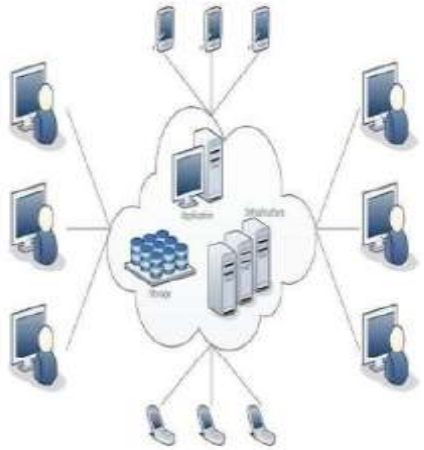

Figure 1: Cloud computing in action.

Distributed computing structure developed from framework registering as in mists are likewise outfit of programming and equipment assets. Advancement however is multidimensional, yet at the same time it is customer and server display. Cloud is perplexing type of utility registering and introduces an unadulterated type of dispersed and parallel.

II. SYSTEM ARCHITECTURE

Mists are normally alluded to as a huge pool of registering and capacity assets, which can be gotten to by means of standard conventions with a unique interface. A four-layer design for distributed computing is appeared in Figure 1.2

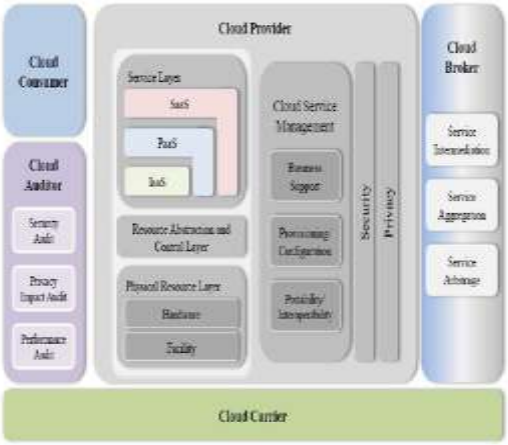

Fig 1.2. Cloud Computing System Architecture.

Types Cloud Deployment Models

Mists are conveyed in various designs, contingent upon the utilization scopes. There are four essential cloud arrangement models.

Public cloud is the standard distributed computing worldview, in which a specialist organization makes assets, for example, applications and capacity, accessible to the overall population over Internet. Specialist co-ops charge on a fine-grained utility registering premise. Cases of open mists incorporate Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google AppEngine and Windows Azure Services Platform. This is a standout amongst the most easy to use and in vogue distributed computing ideal models. Specialist organization provides food registering assets and capacity to cloud client over the Internet based on request. The central element of open cloud is to serve an extensive variety of clients. This model gives the cost-effective administration arrangement over the Internet. According to Gartner enchantment quadrant, worldwide spending for open cloud is expanding generally by 50 percent each quarter.

Hardly any driving open mists are IBM Blue Cloud, Amazon Elastic Compute Cloud (EC2), Google AppEngine, and Windows Azure Services Platform.

Private cloud looks more like a showcasing idea than the conventional standard sense. It portrays an exclusive figuring engineering that gives administrations to a predetermined number of individuals on inner systems. Associations requiring precise control over their information will incline toward private cloud, so they can get all the versatility, metering, and nimbleness advantages of an open cloud without surrendering control, security, and repeating expenses to a specialist co-op. Both eBay and HP Cloud Start yield private cloud organizations. Associations managing touchy information where protection and security are the need over different highlights. It is actualized only for a solitary association or cloud client having a shut system. Focal points of private cloud are adaptability, spryness in addition to control and high security in contrast with an open cloud.

Hybrid cloud utilizes a mix of open cloud, private cloud and even nearby foundations, which is ordinary for most IT sellers. Cross breed procedure is appropriate position of workloads relying on cost and operational and consistence factors. Significant merchants including HP, IBM, Oracle and VMware make suitable plans to use a blended domain, with the point of conveying administrations to the business. Clients can send an application facilitated on a half and half foundation, in which a few hubs are running on genuine physical equipment and some are running on cloud server cases. It is a model shaped by the blend of at least two cloud organization displays among the general population, private and group show. This model possesses quality of the two models like a high financially savvy, better security and high accessibility. Delicate information of association can be taken care of by the private cloud. The confinement of a private cloud can be adjusted by utilizing general society cloud. The test of a half breed cloud is troublesome usage. Organization of mixture engineering is dubious as a result of the divergence.

Community cloud covers with Grids to some degree. It specifies that few associations in a private group share cloud framework. The associations ordinarily have comparative worries about mission, security prerequisites, arrangement, and consistence contemplations. Group cloud can be additionally totaled by open cloud to develop a cross-limit structure. It is a model in which associations having a comparative mission, objective, need, approach, consistence requirements team up to frame a group cloud. Fundamentally numerous associations share cloud framework. Set up is commonly shared among constituting associations having comparable approaches and compliances. Establishments like banks and exchanging firm, share same cloud stage to send applications under high-security contemplations.

Figure 1.3 Cloud Services and Deployment models

THE NEED OF CLOUD ENVIRONMENT

The purposes behind which cloud suppliers and clients are moving to cloud processing are as per the following:

Cloud service outage: There have been various cloud benefit blackout previously. In cloud benefit blackout cloud clients are without administrations gave by cloud suppliers. The cloud clients are urged to possess numerous cases in various datacentres of various areas to achieve continuous administrations, which is money related over set out toward the cloud client. To stay away from cloud blackout Intercloud is a superior choice than single cloud supplier.

Limited scalability: Singular cloud supplier languishes constrained degree over scale out. Keeping in mind the end goal to give better versatility to cloud clients, single cloud suppliers are over provisioning assets. The over provisioned cloud suppliers spend a ton on vitality utilization. So moving to Intercloud is valuable for cloud suppliers as well.

Monitoring: Intercloud gives focal checking administrations and iteratively review status of each cloud parts so as to give consistent support of cloud clients. With better checking rehearses in Intercloud debacle recognition system is progressed than single cloud supplier.

Figure 1.4 speaks to the study done by Rightscale and featured the worries of distributed computing in the years 2016-2017. The chart clarifies the inspiration of cloud clients and suppliers to move to Intercloud from distributed computing.

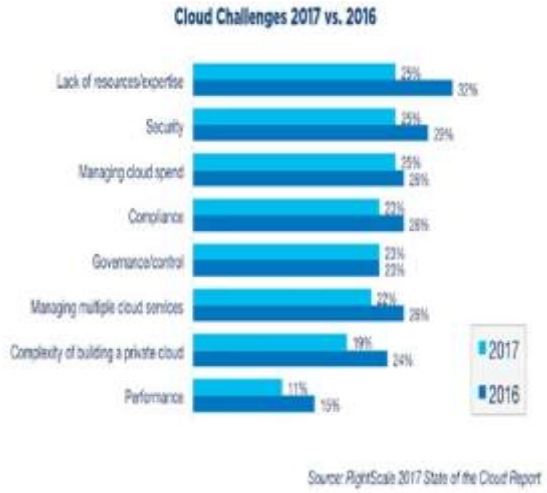

Figure 1.4 challenges of cloud computing which motivates intercloud computing

III. PROBLEM STATEMENT

Cloud computing is defined as global network where resources are shared by across different network and cloud computing offers many services among IaaS (infrastructure as a service), PaaS (Platform as a Service) and SaaS (software as a service) in this work using public cloud and DaaS (Database as a service) are implementing, in general public cloud accessed by everyone like DriveHQ and DropBox are example for public clouds. And using database service any user Maximum 1GB of data he can store in

public cloud. And same way he can access freely across the world. Due to public and global access of cloud the owner need to provide efficient security.

Generally system has multiple owners and users. The owners refer to patients who have full control over their own data, i.e., they can create, manage and delete it. There is a central server belonging to the service provider that stores all the owners‟ s. The users may come from various aspects; like, a friend, a caregiver or a researcher. Users access the documents through the server in order to read or write to someone's, and a user can simultaneously have access to multiple owners‟ data. Correctness of the PHI in the cloud is put at risk due to the following reasons. Although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they still face a broad range of both internal and external threats to data integrity. Outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large scale data storage, it does not offer any guarantee on data integrity and availability. This problem, if not properly addressed, may spoil the successful deployment of the cloud architecture. And the major issues in cloud is Personal health records security and owner un able to controlling his sensitive personal records in cloud storage due to lack of security provided by cloud service provider and the major requirement in cloud computing is access control the owner should enable access control over his data without any issues. Our Proposed work is to improve the privacy preserving framework utilizing Attribute Based Encryption (ABE) with fine-grained approach with precise (accurate) time stamp Server for reliable patient data. Some of the key issues are given mentioned below.

1. Confidentiality is the major issue and providing access control.
2. Owner can't control access polices dynamically.
3. All existing approaches assumed centralized approach where a security key distribution required a trusted party.
4. And owner can't control his cloud storage data
5. If any changes done in attribute polices updating policies will difficult.
6. Attribute revocation will degrade the performance.

IV. METHODOLOGY

This chapter describes the research work carried out with regard to the first objective, the design of the information model and framework of the EHR. The EHR is a systematic collection of health related data about individual patients. The challenge was to develop an open, standardized and interoperable EHR for data representation and information exchange [1]. The data for analysis was collected from PHC in various forms such as existing health records, semi-structured interviews, field notes, and observations. The first study was undertaken to understand the data requirements for a comprehensive EHR in the public health scenario. In the second study, the various standards that could be applied for EHR implementation for public health were studied. To make meaningful use of data represented in health records, the data needs to be seamlessly shared or be interoperable among health care providers [2]. At this juncture, a semantic representation of EHR was adopted to

achieve interoperability and the level of interoperability achieved was also quantified. An XML-based solution for the data sharing or message exchange problem in public health was designed.

Key components

For a health record of an individual to be clinically meaningful, it needs to be created at birth. It should progress through the patient's life and record every clinical encounter or medical event [3]. The essential contents of the EHR for public health were defined based on well-known EHR standards for India, subject expertise and literature. Most EHRs are meant for clinical purposes and they were adapted for public health based EHR. The existing data structures at the RMCWH were also examined [4]. The contents can be classified into various sections meant to capture vital aspects of a patient's health and medical status. The mandatory sections to be included in the EHR structure are as follows:

Patient demographics

The patient demographics section includes details such as name, address, contact numbers, date of birth, sex, marital status, blood group, religion, occupation, location, and emergency contact details. The most important property would be a unique universal medical identifier for the patient. Details of healthcare Financing and medical insurance have to be recorded.

Patient health history and medication

The patients past medical history and present complaint or symptoms need to be captured. Details of immunization the patient has had in his/her life time needs to be captured [5]. Details of any chronic illnesses the patient is suffering from, any known allergies, procedures undergone should also be recorded. The medication prescribed, in terms of brand name, strength of the drug, dosage, duration; route should be available to the doctor. A system by which domain experts can identify the generic ingredient in the medication is required [6]. The various lab tests ordered by the doctor should be recorded and reports such as pathology, radiology, ECG should be stored along with the EHR contents. Multimedia images such as X-ray, MRI, CAT, Ultrasound and Pathology need to be scanned and placed within patients' folders.

Role of standards

Considerable e orts are being put into the standardization of EHRs by different organizations like HL7 and International Standards Organization (ISO) [7]. There are categories of standards, for instance, medical vocabulary standards include Logical Observation Identifiers Names and Codes (LOINC), International Classification of Diseases (ICD10) and Systematized Nomenclature of Medicine-Clinical Terms (SNOMED-CT). There are information model or architecture standards like ISO/TS18308 which specify the requirements for Electronic Health Record Architecture. To study the use of standards for health data exchange, the researchers consider a real world case study of patient referrals.

An electronic referral system is defined to facilitate an effective referral from the rural PHC to a specialist doctor at any hospital or specialist. A scenario where an expectant mother has a medical condition that cannot be treated within the PHC and needs to be referred to the nearest hospital

is considered [8]. The patient details which are currently available in the public health information systems needs to be summarized and sent as an electronic message to the doctor or hospital who will be providing the care. Subsequently, the details of delivery and treatment need to be updated, by the hospital into the PHC records. The solution should be affordable and should ensure seamless data exchange among health care providers and patients. The data exchange should not be affected by technical problems, with regard to the operating platform or database server, etc [9]. The data provided in the referral should be human readable and appropriate for the specialist, to make quality health care decisions [10].

The informal method proposed a series of steps to identify relevant standards. The steps are as follows:

Step 1-Standardization requirement analysis: The standardization requirements should be integrated with SDLC. The various use cases where interoperability is required are identified, and the necessary level of interoperability is also identified.

Step 2- Identification of minimal data set for exchange: The stakeholder groups can identify minimum data sets, considering different scenarios. The data can be represented in the UML-based class diagram.

Step 3- Choosing identifiers: Universal patient identifier needs to be adopted in the form of a URI/IRI. Special identifiers for stakeholders like doctors, ANMs, etc. need to be created.

Step 4- Adoption of vocabularies: Medical vocabularies taxonomies such as SNOMED-CT, CPT, ICD, DICOM, etc. need to be studied to ensure coding of medical conditions. During hospital encounters, the ANMs, doctors or hospitals need to record them against the patient record.

Step 5- Evaluation of existing standards: Standard adopted should be stable, widely accepted, cost-effective and compatible. They should be able to represent the minimal data set required for the application. A simple table to map the concept, attribute in the class diagram to the tags in the standard needs to be created.

V. RESULTS

To develop this application am using DOTNET Technology as a frond technology and SQL server as a backend technology. In .net technology is using IDE as a visual studio with the version of visual studio 2010. And SQL server version with SQL SERVER2008R2.

Entire experiment were carried out in three operations first File encryption and decryption, second File upload third policy update or revoke.

First Operation:

In cloud users uploading file to the cloud in order to that they must generate policy like who can decrypt or not, in below graph policy time calculated for different attributes.

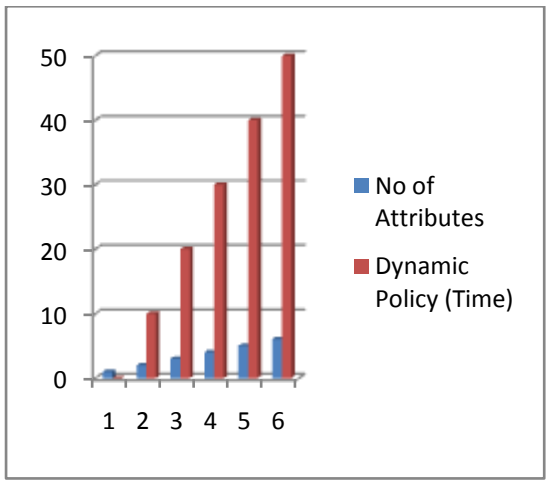

Fig 5.1: Policy generation time

Policy generation done by CP-ABE algorithm in below graph describes comparative time for policy update or revoke for different users calculated.

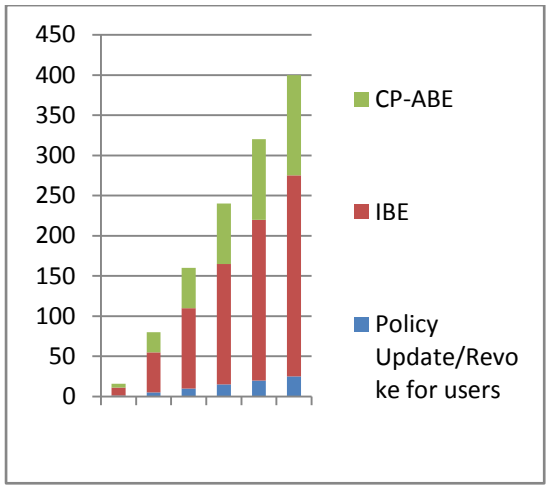

Fig 5.2: Policy update/revoke comparative analysis between IBE and CP-ABE

A user uploading files to dropbox and it allowing users for achieving various functions.To measure the efficiency of different file sizes, data with variable sizes ranging from 100kb to 500kb is selected.

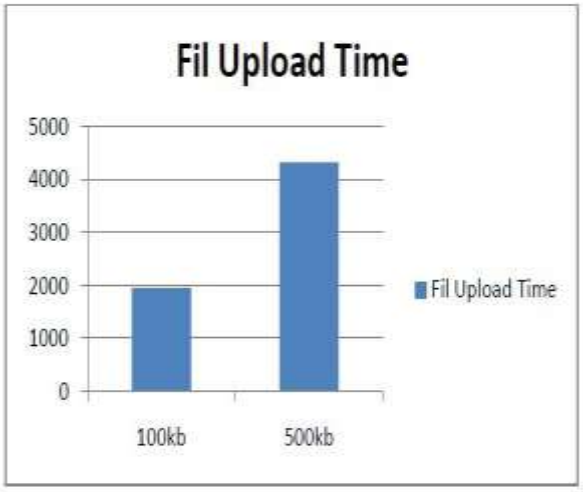

Fig 4.34: File uploads time for different file sizes

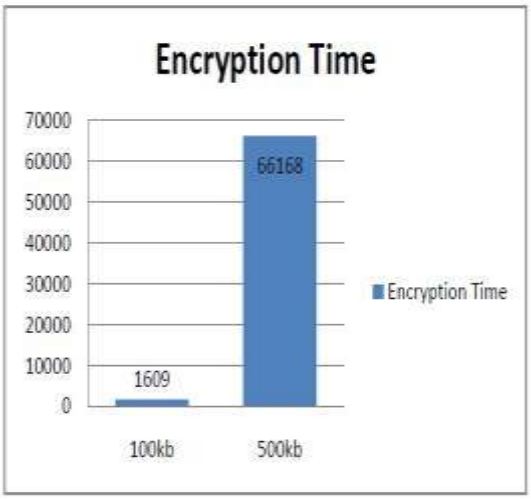

Fig 4.35: File encryption time for different File sizes

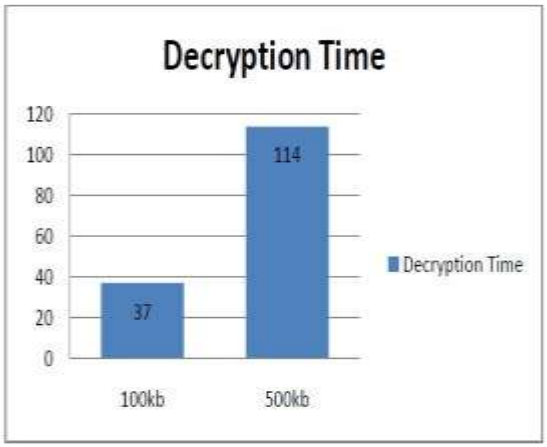

Fig 5.3.: File decryption time for different File sizes

There are many operations are done in this experiment. The users can login and register to the homepage for uploading and downloading the files. The start time for uploading and the finish uploading time is calculated resulting in the total upload time. And same way Encryption and decryption of different file sizes with time calculated.

VI. CONCLUSION

In this work proposed secure framework for personal health records in multi-health care domains where group of doctors and patients share their personal heath records while sharing personal heath records the personal health record owner must be enable access control and policies over cloud shared personal heath records, and the PHR owner can control his data over encrypted cloud data. First PHT owner encrypt he personal heath record under set of policies and he upload to the cloud and doctor or user who want to download the personal health records they first get the secrete key from the owner and they can download the personal health records from cloud after downloading using secrete key they can decrypt but if any policies changes then the cloud owner with help of trusted third party auditor (TTA) will generate new keys to the un revoked users while revoked user secrete key remains same and revoked user can't download the so in this process the TTA will update the attributes when ever user polices changes and data owner can define attributes with time stamp using this a particular user attributes will expiries in certain time period and in this process using asymmetric encryption personal health record will encrypt and keys will distribute to the corresponding to the users via secure channel.

REFERENCES

1. Afnan Salem Babrahem & Muhammad Mostafa Monowar, 2017, "Maintaining security and privacy of the Patient's EHR using cryptographic organization based access control h cloud environment", Intelligent Communication and Computational Techniques (ICCT), 2017 International Conference on, PP: 182-188.

2. Anna Sachinopoulou; et.al, 2007, "Ontology-Based Approach for Managing Personal Health and Wellness Information", ISSN: 1094-687X, Engineering in Medicine and Biology Society, 2007. EMBS 2007. 29th Annual International Conference of the IEEE, PP: 569-571.

3. Alofi Shane Black & Tony Sahama, 2014, "eHealth-as-a-Service (eHaaS): The industrialisation of health informatics, a practical approach", e-Health Networking, Applications and Services (Healthcom), 2014 IEEE 16th International Conference on, PP: 555-559.

4. A. Stolyar; et.al, 2006, "A Patient-Centered Health Record in a Demonstration Regional Health Information Network", Distributed Diagnosis and Home Healthcare, 2006. D2H2. 1st Transdisciplinary Conference on, PP: 160-163.

5. Amin Fallahi; et.al, 2017, "Towards Secure Public Directory for Privacy-Preserving Data Sharing", ISSN: 1063-6927, Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on, PP: 2577-2578.

6. Assad Abbas; et.al, 2015, "A Cloud Based Framework for Identification of Influential Health Experts from Twitter", Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom), 2015 IEEE 12th Intl Conf on, PP: 831-838.

7. Avuya Mxoli; et.al, 2014, "Information security risk measures for Cloud-based personal health records", Information Society (i-Society), 2014 International Conference on, PP: 187-193.

8. Al Amin Hossain; et.al, 2014, "Rapid Cloud Data Processing with Healthcare Information Protection", ISSN: 2378-3818, Services (SERVICES), 2014 IEEE World Congress on, PP: 454-455.

9. Abdul Razaque; et.al, 2016, "Automatic Tampering Detection Paradigm to Support Personal Health Record", Connected Health: Applications, Systems and Engineering Technologies (CHASE), 2016 IEEE First International Conference on, PP: 388-393.

10. Ajmal Sawand; et.al, 2015, "Toward energy-efficient and trustworthy eHealth monitoring system", ISSN: 1673-5447, Volume: 12, Issue: 1, PP: 46-65.