ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 9, March 2018

SECURE STORAGE & DATA STREAMING OF IOT BASED HEALTHCARE DATA : A COMPREHENSIVE VIEW

Shekhara S[1]
Research Scholar
Dept. of Computer Science
Bharathiar University
Coimbatore, TN
sekhar.mysore @gmail.com

P.Raviraj[2]
Professor
Dept. of CSE
GSSS Institute of Engg & Technology for Women, Mysuru
Karnataka
drpraviraj@gmail.com

***Abstract*— The proposed idea deals with the secure database access and control mechanisms in healthcare domain for continuous online Patient-Physician monitoring by using the IoT (Internet of Things) based Multi-Agent systems. The proposed system has the ability to improve health service delivery at the health facilities; more users will have access to medical services right from their smart phones, hence reducing the congestion the health facilities and faster access to services. The health intelligence module works very closely with the database, and executes changes, reminders, notifications, and emergency procedures based on the data. The proposed intelligence sequence is always on alert, investigating all data coming in and out of the system as well as real time monitoring of data that is already stored while referencing it to the in- out data and looking out for patterns and discrepancies. The system will also improve the work of the hospital by offering automated approaches to data collection and analysis, as well as provide a tool for easier more accurate reporting. Once data is updated from one side, it is automatically encrypted and saved using this approach. This system establishes a secure communication between the patient and physician to stay connected at all necessary times; even it also adapted in the of roaming .**

Keywords*— *IoT, Multi Agent System, Secure Communication , Encryption

I. INTRODUCTION

A modernized healthcare system should provide better healthcare services to people at any time and from anywhere in an economic and patient friendly manner. Recent advances in the design of Internet-of-Things (IoT) technologies are spurring the development of smart systems to support and improve healthcare- and biomedical-related process. In a health care monitoring system, it is necessary to constantly monitor the patients physiological parameters. For example a pregnant woman parameters such as blood pressure (BP) and heart rate of the woman and heart rate and movements of fetal to control their health condition.This presents a monitoring system that has the capability to monitor physiological parameters from multiple patient bodies. Sensors have attached on patient body to collect all the signals and sends them to the base station. The attached sensors on patients body are able to sense the heart rate, blood pressure and so on. This system can detect the abnormal conditions, issue an alarm to the patient as well as physician. Through the IoT devices, data collection is automated for vital signs and more sensors can be added to measure environmental conditions in the hospitals that could affect patients. Through the web portable, the medical team is able to view and analyse

collected data that can be used to determine the right course of action towards treating the patients or performing necessary follow up routines hence improving the process of monitoring the patients [1][2][3].

This ability to send messages between the system modules will improve communication between the health facilities and the patients, thus creating an appropriate tool for patient follow up, monitoring and ensuring continuous medical care to the sick. Patients will also be able to send email messages through the app, while the chat feature will allow them to easily get real time communication from health professionals.The appointment feature of the app will make it easier for patients to book appointments with medics, while making it easier for the medics to schedule accordingly, which in turn will lead to streamlined management of patient visits to the health facilities[4][5].

II. SECURE DATABASE AND MESSAGING SYSTEM

The system database is relational and connects to both the user side and medic side, as well as the sensors that are automatically collecting the data; this implies that the data accessed is the same from either end. Once data is updated from one side, it is automatically encrypted and saved as shown in Figure-1. Any information that needs to be transferred is handled through the messaging system that operates closely with intelligence to send out interval messages and notifications based on predefined thresholds or system functions.

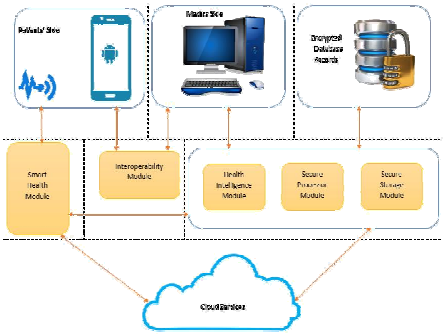

Figure-1: Secure database architecture model for healthcare data

The proposed system has the ability to improve health service delivery at the health facilities; more users will have access to medical services right from their smart phones, hence reducing the congestion the health facilities and faster access to services.

A. Secure Multi Agent Communication System

The proposed architecture is integrated with the secure Multi Agent Communication System for the purpose of establishing a secure communication between the Patient and Physician System. We are using the Multi agent system for the purpose of continuous interaction and making the decision in contact with another agent system that is located in widely spread geographical regions. This would help the patient and physician interaction during the time of travelling or roaming in somewhere else. But the challenging part, we faced is the managing and engaging of all the systems in terms of coordination, cooperation and negotiation of communication. In this proposed system, it provides the password management system to the service agent and the secure agent for the purpose of encryption and decryption. The burden of the user device is reduced because of this encryption and decryption process done by the multi agent system.

The service agent of the communication system serves as an applicant agent for acting as an interface between the Android platform GUI Application and networks. The secure agent played the role like crypto agent, to encrypt and decrypt data and send it back to the service agent. The secure agent uses the AES algorithm for generating a new key every time with the key size of 124Kbytes for the purpose of encryption and decryption process. There is an inbuilt provision assigned to the secure agent for keeping the generated key in the secure storage place. This will helps the patient-physician monitoring and interaction goes in the secured manner. The framework of the secure multi agent communication system is shown in the Figure.2

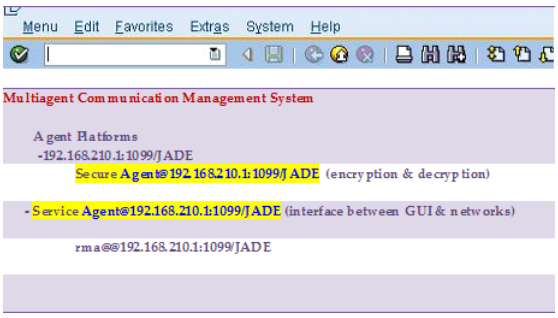

Figure 2. Secured MultiAgent Communication Management System

B. Secure Database Access Control Mechanism

Normally, health care organizations encountered to data regarding unauthorized access to individually identified patient data. To ensure the security, we propose the secure data access technique called as Context-Based Access Control**.** Traditional static access control solutions do not address the complex dynamic security requirements of healthcare applications. For providing secure data access, the proposed context-based access control architecture to fulfill the security requirements of protecting medical data in pervasive healthcare. The system continuously collects and analyses medical data, and updates the access control rules to the data based on the dynamically changing medical condition of the user

We presents the software architecture of our context-*based* healthcare framework. We will also give a detailed description of every component of the architecture.

Context-data Collector and Analyzer: The Context-data Collector and Analyzer (CCA) manages the collection and filtering of context data provided by the context sensor agents, performs analysis on the data, and stores the data into the database.

The Health-data Collector and Analyzer: The Health-data Collector and Analyzer (HCA) manages the collection and filtering of health information provided by the health sensor agents, performs analysis on the data, and stores the data into the database. Based on the collected data, the HCA might also trigger events such as dialling or raising some warnings to get the attention of the data owner or the medical service provider to some concerns with the medical data.

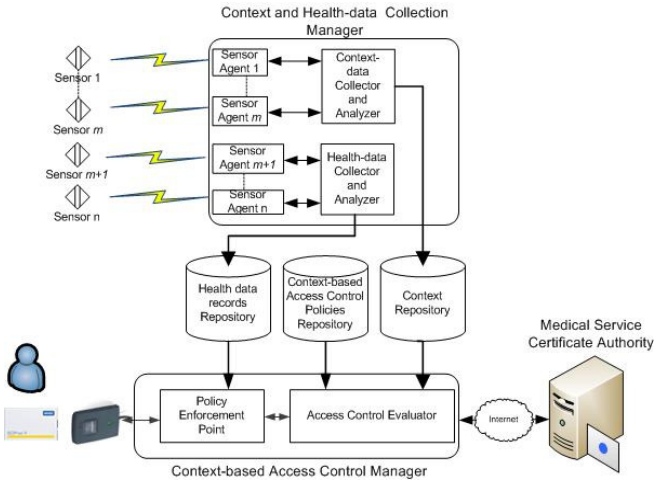

Figure-3 : Working mechanism of Context based access control manager

The Context-based Access Control Manager: The Context-based Access Control Manager (CASM) acts as a Policy Decision Point (PDP) and a Policy Enforcement Point (PEP) for the system. It receives requests from the applications to access the health data, authenticates the identity of the data requestor, uses the data in the context database, and evaluates the access control policies stored in the policy repository to decide whether to grant or deny requests. The decision is passed to a Policy Enforcement Point (PEP) for enforcement. The working mechanism is as shon in Figure-3

Access Control Evaluator: The Access Control Evaluator (ACE) is the policy decision point in the system. When an application makes a request to the system to access the data in the database, the ACE contacts the certificate authority of the medical service provider to evaluate the identity of the requestor, and uses the context information to retrieve the policies in the database that apply to the current context. The decision to grant/deny access to the data is passed to the policy enforcement point for implementation.

Policy Enforcement Point: The Policy Enforcement Point (PEP) is the logical entity that accepts the request from an application that tries to access health data in the system, and

passes the request to the ACE. When the ACE makes a decision, it passes this decision to the PEP to enforce it.

The Database System: The system requires the usage of three databases: a Health-data Repository, a Context-data Repository, and an Context-based Access Policy Repository.

Health-data Repository: The Health-data Repository (HR) stores the health data generated by the health data collector and analyzer. This data consists of the medical history of the person to which the medical sensors are attached. Such data might include electrocardiogram data, heart beat information, and blood pressure, to list a few.

Context data Repository: All the context information is stored in the Context-data Repository by the context data collector and the Analyzer. This data will help the ACE to make its decision based on the current state of the system.

Context-based Access Policy Repository: The Context-based Access Policy Repository database stores the context policies which are used in combination with the context data record to grant/deny access to the user's health data.

Service Provider Certificate Authority: The Service Provider Certificate Authority is responsible to issuing certificates such as from an RFID card to the paramedic. It is also responsible for confirming that the paramedic is on duty when he/she is trying to access the medical data of the user.

C. Context Based Data Assess Scheme

Context-based access control takes into account the person attempting to access the data, the type of data being accessed and the *context* of the transaction in which the access attempt is made. With the foregoing in mind, here are the core principles on which the proposed context-based access control model is based:

(i) All PHI is maintained in relational database tables.

(ii) Access to PHI tables is allowed only via stored procedures.

(iii) Each stored procedure contains context-based access control logic.

The sample coding for context based access control are as follows.

```
rem  Get  the  key  for  the  current  user.

          SELECT  primary-key  INTO  doctor-key
          FROM  USER
          WHERE  user-name  =  user;

rem  Get  the  key  for  the  patient  in  question.

          SELECT  primary-key  INTO  patient-key
          FROM  SUBJECT_INDIVIDUAL
          WHERE  patient-name  =  patient;

rem  Look  up  the  "treatment"  type  code.


                SELECT  primary-key  INTO  relationship-
                type
                FROM  RELATIONSHIPS
                WHERE  relationship-name  =  "TREATMENT";

 rem  Get  a  count  of  affiliation  rows  of  this  type.

                SELECT  COUNT(*)  into  rowcount
                FROM  AFFILIATION
                WHERE user-key = doctor-key AND
                      subject-individual   -key
                      =     patient-key     AND
                      affiliation-type        =
                      relationship-type;

      rem  Allow  the  access  if  there  is  at  least  one  such  row.

      IF  (rowcount   0)  {
      allow  =  TRUE;
                } ELSE  {
      allow  =  FALSE;
                }

                RETURN(allow);

           END;
```

III. EXPERIMENTAL RESULTS

Before leaving the description of the model, We would like to reemphasize the dependency of the model on core operating system and database security controls. For the model to be properly implemented all application tables, and the stored procedures used to access the tables, should be owned by a userid for which the log-in privilege has been disabled. Users should be granted access to the procedures needed to accomplish their assigned job functions but no one should be granted access to the tables themselves. Finally, all

invocations of the stored procedures should be done in the context of valid user database sessions.

The administrator refers to people who are responsible for managing and maintaining the database and web system. Administrator has full capability to access all information in the web-based application. Administrator is responsible to create new account for other administrators, doctors and patients. Doctors and patients have limited capability to access the database compared to administrator. Table-1,2,3,4 & 5 are showing the context based mapping and its accessing results as below.

Table 1 : The capability of each user to access the web-based

	Administrator	Doctor	Patient
Add/Edit Doctor Information	Yes	No	No
Add/Edit Patient Information	Yes	Yes	No
View Medical Signal	Yes	Yes	Yes
Add/Edit Comment	Yes	Yes	Yes
Read Comment	Yes	Yes	No
View Patient Information	Yes	Yes	No

Table 2 - Subject-Domain Mapping

Subject	**Domain**	**Predicate**
Admission_proc	patient_mgmt_domain	Subject_Domain(admission_proc, patient_mgmt_domain)
Discharge_proc	patient_mgmt_domain	Subject_Domain(discharge_proc, patient_mgmt_domain)
Transfer_proc	facility_mgmt_domain	Subject_Domain(transfer_proc, facility_mgmt_domain)
lab_orders_proc	care_provider_domain	Subject_Domain(lab_orders_proc, care_provider_domain)

Table 3 - Domain-Type Access Matrix

Domain	**Object-Type / Access Modes**		
	Patient Registration Type	**Patient Location Type**	**Patient Clinical Type**
Patient_mgmt_domain	C, U, D,V	D, V	
Facility_mgmt_domain		C,U,V	
Care_provider_domain	V	V	C, U, V

Access Mode Codes: C – Create , U – Update, D – Delete , V – View

Table 4 - Menu Option to Context Variable Mapping in ADT

Menu Option	**Context Variable (CV)**
1. Admit Patient	NONE
2. Change Beds/ Room	wardname
3. Transfer to Acute Care	facilitytype
4. Order Lab Tests	patientname
5. Discharge Patient	NONE

Table 5 - Menu Option to Context Variable Mapping in ADT

Ward	Administrator	Predicate
PEDIATRIC	smith	Ward_Assignment(smith,'PEDIATRIC)
MATERNITY	mell	Ward_Assignment(mell,'MATERNITY')

IV. CONCLUSION

Thus the proposed idea carried out the analysis of data collected, created a baseline for the entire database and delivered critical information that was necessary for the actual design and implementation of the system. The system design took into account data collected during research in order to come up with a system that addresses the needs of the target population. The entire purpose of this context-based access control system is to prevent unauthorized parties from viewing the personal medical information of the patient. While we have assumed that the data will be stored in a secure manner and all transactions will also be secure, our architecture would benefit greatly by including mechanisms for encryption and decryption as well as a digital-signature system to guarantee non-repudiation of transactions

REFERENCES

[1] Goyen, M., & Debatin, J. F. (2009). Healthcare costs for new technologies. *European journal of nuclear medicine and molecular imaging*, *36*(1), 139-143.

[2] Lanseng, E. J., & Andreassen, T. W. (2007). Electronic healthcare: a study of people's readiness and attitude toward performing self-diagnosis. *International Journal of Service Industry Management*, *18*(4), 394-417

[3] Marien, M. (2010). Futures-thinking and identity: why "Futures Studies" is not a field, discipline, or discourse: a response to Ziauddin Sardar's 'the namesake'. *Futures*, 42(3), 190-194.

[4] Kummervold, P. E., Chronaki, C. E., Lausen, B., Prokosch, H. U., Rasmussen, J., Santana, S., ... & Wangberg, S. C. (2008). eHealth trends in Europe 2005-2007: a population-based survey. *Journal of medical Internet research*, *10*(4).

[5] Fernandez, F., & Pallis, G. C. (2014). Opportunities and challenges of the Internet of Things for healthcare: Systems engineering perspective. In *Wireless Mobile Communication and Healthcare (Mobihealth), 2014 EAI 4th International Conference on* (pp. 263-266).