Health Care Monitoring System Using Android Application (IOT)

R.Ramya[1], G.Nivetha[2], M.Soundarya[3]
[1]Assistant Professor, DEPT OF Computer Science And Engineering
[2, 3]DEPT OF Computer Science And Engineering
[1, 2, 3] JEPPIAAR SRR Engineering College, Chennai, TN

Abstract- *Tele monitoring systems face the problem of delivering medicine to the current growing population with chronic conditions while at the same time covering the dimensions of quality of care and new paradigms such as empowerment can be supported. By periodically collecting patients themselves clinical data and transferring them to physicians located in remote sites, patient's health status regulation and response provision are possible. This type of telemedicine system guarantees patient control while reducing costs. So, to avoid hospital overflows we proposed the design and implementation of an architecture based on the combination of ontology rules, web services, and the autonomic computing paradigm to manage data in home -based telemonitoring scenarios. This ontology -based solution defines a flexible and scalable architecture in order to address main challenges presented in home-based telemonitoring scenarios and thus provide a means to integrate, unify, and transfer data supporting both clinical and technical management task.*

Keywords- Body Sensor Network (BSN) Secure and privacy preserving oppurnustic (SPOC) personal Health care Information (PHI) Smart Message Service (SMS)

I. INTRODUCTION

IN our aging society, mobile Healthcare (m-Healthcare) system has been envisioned as an important application of pervasive computing to improve health care quality and save lives, where miniaturized wearable and implantable body sensor nodes and smart phones are utilized to provide remote healthcare monitoring to people who have chronic medical conditions such as diabetes and heart disease. Specifically, in an m-Healthcare system, medical users are no longer needed to be monitored within home or hospital environments. Instead, after being equipped with smart phone and wireless body sensor network (BSN) formed b body sensor nodes, medical users can walk outside and receive the high-quality healthcare monitoring from medical professionals anytime and anywhere propose a new secure and privacy preserving opportunistic computing framework, called SPOC, to address this challenge With the proposed SPOC framework, each medical user in emergency can achieve the user-centric high-reliability of PHI process and minimizing PHI privacy disclosure in m-Healthcare emergency

II. EXISTING SYSTEM

C. Jr. Arcadius Tokognon, Bin Gao; They first identified some unique design requirements in the aspects of security and privacy preservation for communications between different communication devices in vehicular *ad hoc* networks. Then they proposed a secure and privacy-preserving protocol based on group signature and identity (ID)-based signature techniques. They have demonstrated that the proposed protocol cannot only guarantee the requirements of security and privacy but can also provide the desired traceability of each vehicle in the case where the ID of the message sender has to be revealed by the authority for any dispute event.

R. Lu, X. Lin, X. Liang This problem of storing and executing an application that exceeds the memory resources available on a single node. The proposed solution is based on the idea of partitioning the application code into a number of opportnusticistically cooperating modules. Each node contributes to the execution of the original application by running a subset of the application tasks and providing service to the neighbouring nodes

Y.Ren, Pazzi presented several techniques that can be used to monitor patients effectively and enhance the functionality of telemedicine systems, and discussed how current secure strategies can impede the attacks faced by wireless communications in healthcare systems and improve the security of mobile healthcare.

R. Lu, X. Lin, The above author discussed the evolution from opportunistic networking to opportunistic computing; they survey key recent achievements in opportunistic networking, and described the main concepts and challenges of opportunistic computing .they finally envision further possible scenarios and functionalities to make opportunistic computing a key player in the next-generation Internet.

Y. Zheng, stated that 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 leveraged attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, they focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users.

M.R.Yuce,.Khan and above authors presented analytical model that depicts the service invocation process between seekers and providers. Specifically, they derive the optimal number of replicas to be spawned on encountered nodes, in order to minimize the execution time and optimize the computational and bandwidth resources used. Performance results show that a policy operating in the optimal configuration largely out performs policies that do not consider resource constraints.

2.1 LIMITATION OF THE EXISTING SYSTEM

Ontology provides a higher level of abstraction and has been successfully used in telemonitoring scenarios and other areas to provide knowledge representation and semantic integration, thus a common understanding about data exchanged by all the entities.

It maintains two layers they are the conceptual layer deals with data representation and includes the ontology for interpreting the data transferred for the communication of end sources of the architecture. The data and communication layer deals with data management and transmission.

III. PROPOSED SYSTEM

The architecture diagram for the proposed system is represented in the figure. we have a tendency to propose a replacement secure and privacy protective opportunist computing framework, known as SPOC, to handle this challenge. With the planned SPOC framework, every medical user in emergency are able to do the user-centric privacy access management to permit solely those qualified helpers to participate within the opportunist computing to balance the high-reliability of letter method and minimizing letter privacy speech act in m-Healthcare emergency. Specifically, the most contributions of this paper area unit threefold.

First, we have a tendency to propose SPOC, a secure and privacy-preserving opportunist computing framework for mobile-Healthcare emergency. With SPOC, the resources accessible on different opportunistically contacted medical users' smart phones will be gathered along to manage the computing intensive letter method in emergency scenario. Since the letter are $^{\text{disclosed}}$ throughout the method in opportunist computing, to attenuate the letter privacy speech act, SPOC introduces a user-centric two-phase privacy access management to solely enable those medical users UN agency have similar symptoms to participate in opportunist computing.

Second, to realize user-centric privacy access management in opportunistic computing, we have a tendency to gift associate economical attribute based access management and a unique non-homomorphism cryptography primarily based privacy-preserving inner product computation (PPSPC) protocol, wherever the attributed-based access management will facilitate a medical user in emergency to spot different medical users, and PPSPC protocol will additional management solely those medical users UN agency have similar symptoms to participate within the opportunist computing whereas while not directly revealing users' symptoms.

Third, to validate the effectiveness of the planned SPOC framework in m-Healthcare emergency, we have a tendency to conjointly develop a custom machine inbuilt Java. Intensive simulation results show that the planned SPOC framework will facilitate medical users to balance the high-reliability of letter method and minimizing the letter privacy speech act in m-Healthcare emergency

3.1 ADVANTAGE OF THE PROPOSED SYSTEM

1) Our proposed architecture to enhance its effectiveness and improve its functionalities to handle Maps.
2) Provide member based patients-monitoring that is trusted patients can only use this system.
3) Representational state transfer (REST) style and based on a generic communication method, provides a different design approach that may be reusable for other systems based on ontology's.

3.2 ARCHITECTURE DIAGRAMG

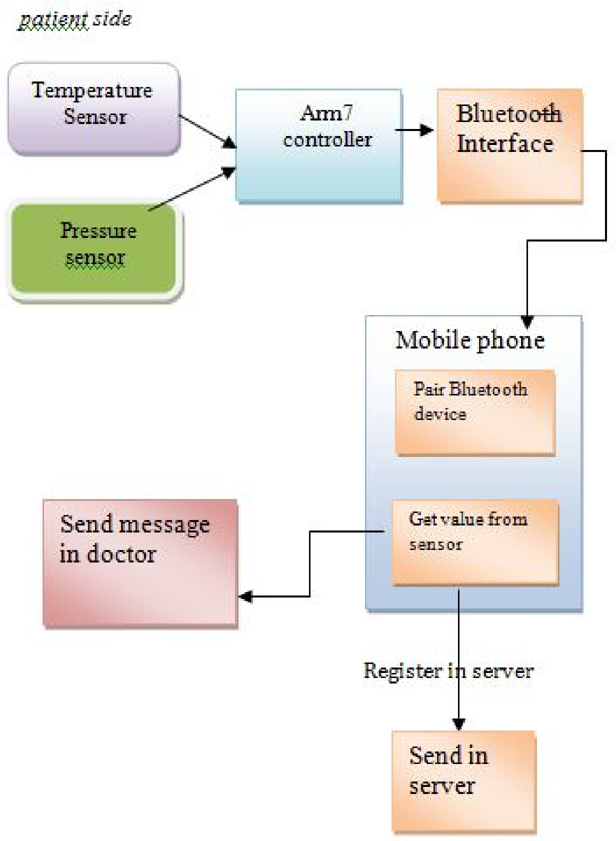


Fig 1 Architecture diagram for patient side

By periodically collecting patients themselves clinical data and transferring them to physicians located in remote sites, patient's health status regulation and response provision are possible. This type of telemedicine system guarantees patient control while reducing costs. So, to avoid hospital overflows we proposed the design and implementation of an architecture based on the combination of ontology, rules, web services, and the autonomic computing paradigm to manage data in home-based telemonitoring scenarios.

Server side

1) The proposed architecture includes three layer: the theoretical layer (the ontology) the communication and data layer and the tragedy alert layer
2) Theoretical layer includes both the ontology and the the definition of rules In particular, rules are used in combination with the ontology to provide personalized services
3) 3) The second layer is based on WSS technologies. WSS have been successfully used in network management and also in other works to exchange data modeled by ontology
4) Tragedy alert layer is based on patients health data.if patients health data critical means it will generates alarm

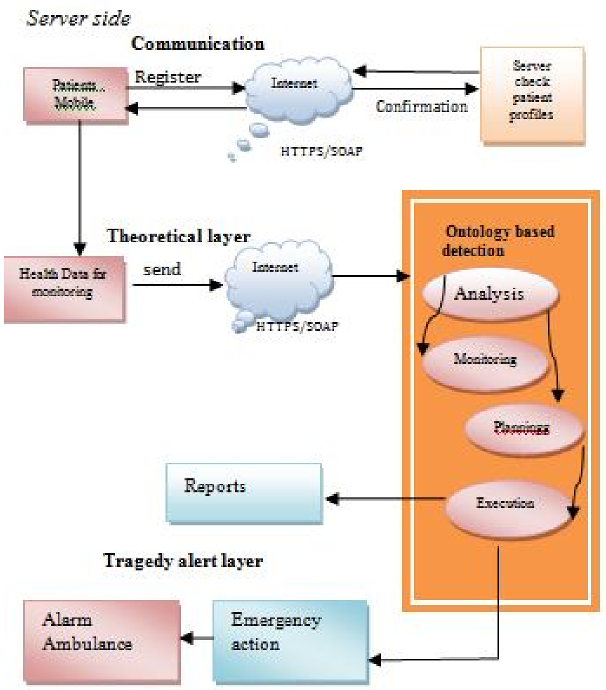


fig-2 *Architecture diagram for server side*

IV. MODULES DESCRIPTION

LIST OF MODULES

1. Monitoring the patient
2. Embedding the body sensor
3. Transmission of values
4. Sending alert message

4.1.1 Monitoring the patient

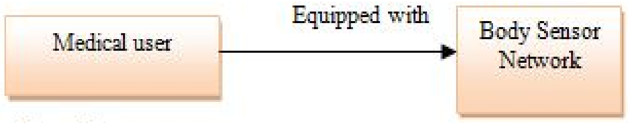
Normally the medical user personal healthcare information (PHI) is mainly invented for monitoring the patients without direct interaction with doctors. In an mobile Healthcare system, medical users no longer needed to monitored within home or hospital environments. Instead, after being equipped with smart-phone and wireless body sensor network (BSN) formed by body sensor nodes, medical users can walk outside and receive the high-quality healthcare monitoring from medical professionals anytime and anywhere.

Algorithm

1) Start.
2) Monitor the patient temperature and pressure at residing place.

3) Use sensor to monitor the patient condition

4.1.2 Embedding the body sensor



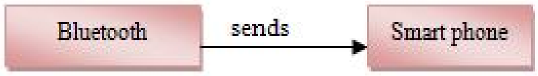
Algorithm

1) Start.
2) Provide a body sensor to the medical user.
3) Transmit the user details using sensor.
4) Stop.

This sensor will be equipped directly in the medical user. This BSN will transmit the user details for every time period that we have indicated. For example, each mobile medical user's personal health information (PHI) such as heart beat, blood sugar level, blood pressure and temperature and other details will be captured by the medical users Smartphone.

.

4.1.3 Transmission of values



Algorithm

1) Start.
2) Interface the temperature and pressure using Arduino board.
3) Send the values to the Bluetooth from the body sensor.
4) Pair the Bluetooth to the smart phone.
5) Finally send the values to the smart phone.
6) Stop.

For each data transmitted from BSN will be aggregated by the Smartphone that, the medical users having with them using Bluetooth communication. This received medical information or symptom will be transmitted to healthcare center periodically with the help of 3G network

.4.1.4 Sending alert message

Mobile
Sends
Healthcare center
alert
Patient

A Secure and privacy-preserving opportunistic computing (SPOC) framework for mobile-Healthcare emergency. With SPOC, the resources available on other opportunistically contacted medical users' smart-phones can be gathered together to deal with the computing-intensive PHI process in emergency situation. Since the PHI will be disclosed during the process in opportunistic computing, to minimize the PHI privacy disclosure, SPOC introduces a user-centric two-phase privacy access control to only allow those medical users who have similar symptoms to participate in opportunistic computing.

Algorithm

1) Start.
2) Send the values to the server using the 3G or any other network.
3) The server receives the user values.
4) The server sends the alert message to the user if he/she is abnormal.
5) Stop.

V. CONCLUSIONS

This mainly exploits how to use opportunistic computing to achieve high reliability of PHI process and transmission in emergency while minimizing the privacy disclosure during the opportunistic computing. Detailed security analysis shows that the proposed framework can achieve the efficient user-centric privacy access control. In addition, through extensive performance evaluation, we have also demonstrated the proposed framework can balance the high-intensive PHI process and transmission and minimizing the PHI privacy disclosure in m-Healthcare emergency.

REFERENCES

[1] C. Jr. Arcadius Tokognon, Bin Gao, Senior Member, IEEE, Gui Yun Tian, Senior member,'' Structural Health Monitoring Framework Based on Internet of Things, IEEE, and Yan Yan , 2017

[2] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Handshake with Symptoms-Matching: The Essential to the Success of mobile healthcare Social Network," Proc. Fifth Int'l Conf. Body Area Networks (Body Nets '10), 2010

[3] Y. Ren, R.W.N. Piozzi, and A. Boukerche, "Monitoring Patients via Secure and Mobile Healthcare System," IEEE Wireless Comm.,vol. 17, no. 1, pp. 59-65, Feb. 2010.

[4] R. Lu, X. Lin, X. Liang, and X. Shen, "A Secure Handshake Scheme with Symptoms-Matching for mobile Healthcare Social Network "Mobile Networks and Applications—special issue on wireless and personal comm., vol. 16, no. 6, pp. 683-694, 2011.

[5] M.Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud

Computing Using Attribute-Based Encryption," IEEE Trans. Parallel and Distributed system, vol. 31, no. 6,pp. 432-438,Feb 2012