

Secure Health Monitoring and Predictive System Using Cloud Computing

***Omkar Khot, Abhishek Basagare, Vahid Mujawar, Jeenika Anadani, Rohini Mali*,
Mahesh P. Gaikwad***

Sanjay Ghodawat Group of Institutions, Atigre (India)

Corresponding author's email id: rohinimali321@gmail.com *

DOI: <http://doi.org/10.5281/zenodo.2641622>

Abstract

Security, in information technology is the shield of statistical knowledge and IT assets against centralized and outmost, vicious and unexpected hazards. Security is demanding for enterprises and organizations of all sizes and in all industries. Weak security can result in compromised systems or data, either by a vicious hazard actor or an unintentional internal hazard. Now-a-days healthcare business is growing tremendously due to the increase in elderly population and decline in birthrate. A healthcare becomes a big concern due to lack of opportunity of expert doctors. Due to this concern there is a paradigm shift from need based health monitoring to preventive health monitoring service. Keeping in view this scheme we are proposing a health care system which will be unified with cloud computing. That will make system adept of generating EMR i.e. Electronic Medical Records of patients which will play a favorable role for patient's diagnostic and speedy gain process as well as for medical practicing doctors who need vast medical cases for their own study purpose. This system will keep track of patient's health in a timely manner and generate a alert when the patient's vital parameters crosses the normal value. This paper focuses on a health care monitoring with security

Keywords: *Security, Navigation, Global Positioning System, Cloud, Geo-location, Augmented Reality*

INTRODUCTION

A crucial improvement is the strength to join such devices to large capital pools such as cloud. The combination of encapsulated devices and cloud servers offers wide pertinence of IoT to many areas of our life. With the stale population expanding every day, encapsulated devices with cloud server can provide the elderly with more adjustable service without the need to visit hospitals.

The layout and combination of security burden, like verification and data hiding for establishing the elderly privacy, need to be taken into deliberation. An intelligent and secure health monitoring scheme using security and data science using cloud computing and cryptography is planned. The planned scheme enacts verification and provides crucial security need. For many healthcare applications, having a straight forward sensor-to-cloud architecture is not feasible, exclusively due to the certainty that most hospitals would not prefer patient data to be hoarded exterior [3]. Thus in this project as the patient data will be hoarded inward a cloud and will be secured terribly there is very limited risk of data being discovered to exterior party.

Cloud based health monitoring system is used for a bold approach in the contemporary life. Exclusively old patients should be systematically monitored and their loved persons need to apprise about their health condition at that time. If system disclose any abrupt shift in patient, then it signal's the user and their family member.

We provide the security for the given data and analyze that data and predict the health of the patient given to the server.

LITERATURE SURVEY

An aging society refers to a population structure Model in which the aging population reaches or exceeds a certain proportion. According to the UN's traditional standard a region is regarded as an aging society when people over 60 years old account for 10% of the total population, while the new standard is people over 65 years old representing 7% of the total population. Between 2015 and 2050, the proportion of the world's population over 60 years will nearly double, from 12% to 22% [1]. Wireless sensor networks (WSNs) are an emerging technology that possesses a huge potential to play an important role in many applications [4] flexibility, scalability, and heterogeneous information services. The

integration of WSN with cloud provides greater flexibility, unlimited resources, immense processing power, and the ability to provide quick response to the user [6]. Many studies [3, 9] pointed out that cloud computing services are clearly the future trend. Cloud computing services are provided through a browser to access online programming applications, software, and data [9]. Cloud providers have to adhere to security and privacy policies to ensure their users' data remain confidential and secure [10]. For many healthcare applications, having a simple sensor-to-cloud architecture is not viable, especially due to the fact that most hospitals would not prefer patient data to be stored outside [3]. In recent years, many medical resources have been implemented for people seeking medical advice conveniently [11]. In the literature [12], researchers combine mobile devices and body sensors but do not sufficiently

discuss security issues. In 2014, Ben Othman et al. proposed an efficient solution for securing data transmission, which combines compressive sensing with encryption and integrity checking [16]. In 2015, an ECC-based mutual authentication protocol for secure communication between embedded devices and cloud servers was presented in a paper by Kalra and Sood [17].

PROPOSED WORK

Thus in this project we are ensuring security on both server and client end. We are also going to analyze the health of patients in a graphical manner for easy understanding and also predict the health for what can happen with symptoms. Senior citizens find it difficult to go all the way to hospital and we are also making sure to send an ambulance if at all there is a worst case.

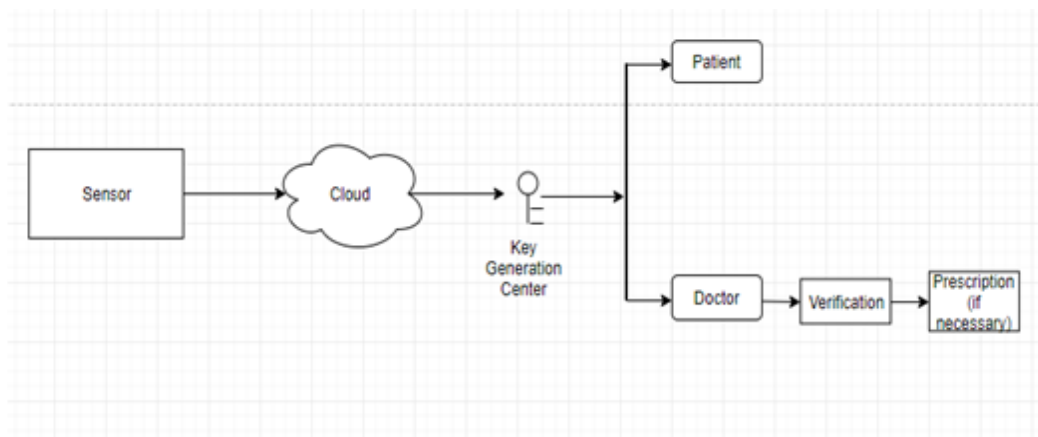


Figure:-1

SYSTEM ARCITECHTURE

The systems architecture will be broken up into 4 parts. While each of these parts can be seen as separate systems, each part does form part of the healthcare monitoring system.

A. HealthCare Sensing

The measuring of a patient's health information would be done in the rural village of the patient where there is no access to medical professionals and vitals measuring equipment. The measuring of these vital parameters would have to be done by the patient using the system. The system would have to accommodate for the computer skills of the people using it. The data for this section of the project would all be "faked" at this point. Time constraints prevent us from getting ethical clearance for doing the actual monitoring ourselves. An investigation is still underway to determine if we can link with other researchers in who might be undertaking the task of monitoring and recording patient data.

B. Security and Privacy

Since the nature of the data is medical we suggest that all communications within the system should be over encrypted network channels. This will ensure protection against integrity attacks and

communication interception. The communications between the wireless smart boards (ALIX boards) and the data store/database will also be encrypted. Access to the database of medical data should also be by only authorized medical personnel and the ALIX boards, which requires us to set up a security policy on database access and transactions.

C. Middleware and Database

Dissemination would occur at multiple entry points. This could be either via public IP access meaning devices with internet connectivity can be connected directly possibly giving live updates of data. This entry point can also be used to connect to remote grids that only have periodic internet access or to extend the grid to new sites that have permanent internet connectivity. This public access however requires security controls to ensure data being sent is from authorized systems and that new systems wishing to join are clearly identified as being uncompromised and trustworthy nodes, as such nodes could insert data which could negatively impact the analysis of data in decision making processes.

D. Front End application

The front end application will serve as a dashboard for medical professionals to

check up reports on their patients. It will also serve as a notification center for medical professionals to monitor critical patients. The proposed system focuses on collection of patient's vital health parameters and generates alert to care takers, doctors so that immediate action can be taken in case of emergencies. The data is then stored in Cloud so that data can be accessed via Internet from anywhere anytime. Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over the network (mainly the Internet). Cloud has abundant processing power, large amount of storage which can be scaled according to application needs. Modern technology is being shifted to Cloud based platform as it is suited for long-term data storage.

In our scheme, each party should register at the key generation center which will issue a pair of public key and private key, to communicate with other parties. The user also gets the pre generated key; it can be used to encrypt the private health information. The elders can use a mobile device to connect to the IoT medical sensor which can collect the biological data. Seven parties are involved in our scheme as follows.

(1) Elder (E). The aging population with chronic disease (e.g., heart disease, diabetes, and hypertension) wears the IoT medical sensor which can collect biological data.

(2) Cloud (C): Intelligent Data Storage. The elder can access the cloud service to upload/download the health information via authentication. It can provide smart applications and send private health reports to the elder at set periods of time. Once there is an emergency situation, the cloud will notify the hospital.

(3) Hospital (H) It is a hospital where the elder can get physical inspection and the report. Once the elder's biological data are over a threshold, the hospital will notify the elder and dispatch an ambulance after it gets the cloud's notification.

(4) Key Generation Center (KGC) The key generation center will issue a pair of public key and private key for the registered parties. The user's pre generated key and the time of the key's generation are stored in the database.

(5) IoT Medical Sensor (MS) It is the collecting device of the elder's biological data. The IoT medical sensor can also.

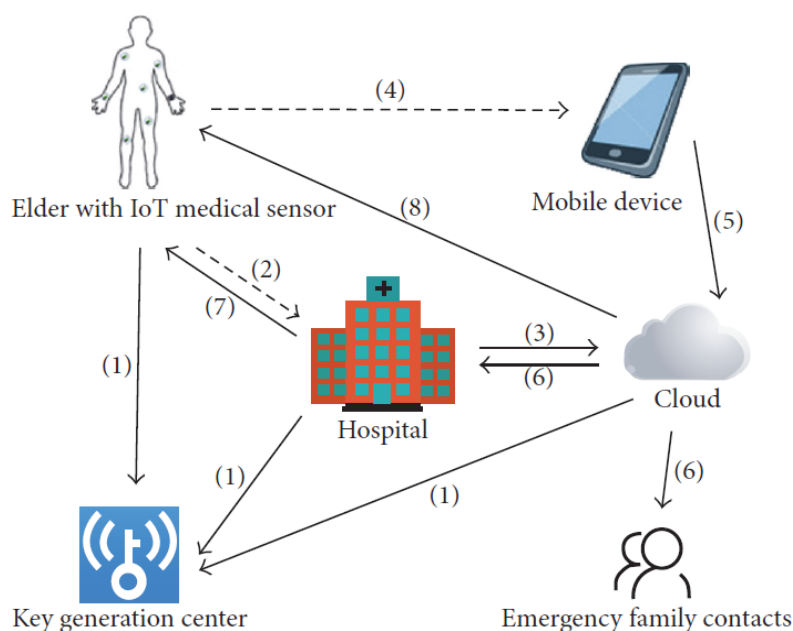


Figure:-2 The system architecture

1. The elder, the hospital, and the cloud must register at the key generation center in advance via secure channel.
2. The elder goes to hospital for a physical inspection.
3. The hospital uploads the elder's physical inspection report to the cloud.
4. The IoT medical sensor gets the elder's biological data via set periods of time and sends it to the mobile device.
5. The mobile device uploads the biological data to the cloud.
6. The cloud compares the data sent from the mobile device with the standard values stored in the database. Once there is an emergency, the cloud notifies the hospital and contacts the elder's family in an acceptable time.
7. After the hospital gets the notification, it sends messages and dispatches an ambulance to the elder.
8. If the data collected by the IoT medical sensor are normal, the cloud sends a health report to the elder at set periods of time.

DIFFERENT PHASES

The Hospital Uploads Physical Inspection Report Case.

The elder goes to the hospital for a physical inspection. After the hospital and the cloud process authentication, the hospital uploads the physical inspection

report to the cloud. The flowchart of the hospital uploading physical inspection report case

The Mobile Device Uploads Biological Data Case.

In this phase, we consider the IoT medical sensors embedded into an elder's body. The elder uses the mobile device to transfer the biological data which are measured by IoT medical sensors to the cloud.

The Emergency Case

When the cloud gets the elder's biological data from the mobile device, the cloud compares the data with the standard values stored in the database. If there is an emergency situation, the cloud sends the alert message to the hospital and contacts the emergency family simultaneously. Then, the hospital will contact the elder and dispatch an ambulance to help the elder, if necessary.

CONCLUSION

AR Navigation is undeniably a resource which can make a navigation system more intuitive and user friendly. People can use their mobile phone's camera to experience the same. Users can also setup a camera device for the same purpose. An attempt has been made to replace the current

navigation systems which are seen in the low end cars. The POIs have been set up and classified according to their types. Real time AR can help the user to easily traverse through the city by obtaining various alerts such as uneven roads or accidental prone areas. The navigation system using AR can be considered as more efficient than traditional navigation system as it may provide the user with the virtual path through the camera itself. Further enhancements can be achieved by implementing the same in the windshield of the car. The system can be developed as an Android/iOS application which can help any user to navigate easily. The elder's continuous medical monitoring is a serious problem. In this paper, we proposed a scheme with IoT sensor based on cloud computing to make the elder safely and conveniently monitored. In our scheme, the digital envelope, digital certification, signature, and timestamp mechanisms are involved.

REFERENCES

1. World Health Organization, <http://www.who.int/mediacentre/>
2. H. J. La, H. T. Jung, and S. D. Kim, "Extensible disease diagnosis cloud platform with medical sensors and IoT devices," in

- Proceedings of the 3rd International Conference on Future Internet of Things and Cloud (FiCloud '15), pp. 371–378, IEEE, Rome, Italy, August 2015.
3. Z. Zhang and X. Hu, “ZigBee based wireless sensor networks and their use in medical and health care domain,” in Proceedings of the 7th International Conference on Sensing Technology (ICST '13), pp. 756–761, Wellington, New Zealand, December 2013.
4. C.-L. Chen, T.-T. Yang, M.-L. Chiang, and T.-F. Shih, “A privacy authentication scheme based on cloud for medical environment,” *Journal of Medical Systems*, vol. 38, article no. 143, 2014.
5. Hendre and K. P. Joshi, “A semantic approach to cloud security and compliance,” in Proceedings of the IEEE 8th International Conference on Cloud Computing (CLOUD '15), pp. 1081–1084, New York, NY, USA, June 2015.
6. C.-L. Chen, T.-T. Yang, and T.-F. Shih, “A secure medical data exchange protocol based on cloud environment,” *Journal of Medical Systems*, vol. 38, no. 9, article 112, 2014.
7. S. Ben Othman, A. Trad, and H. Youssef, “Security architecture for at-home medical care using Wireless Sensor Network,” in Proceedings of the 10th International Wireless Communications and Mobile Computing Conference (IWCMC '14), pp. 304–309, IEEE, Nicosia, Cyprus, August 2014.
8. S. Kalra and S. K. Sood, “Secure authentication scheme for IoT and cloud servers,” *Pervasive and Mobile Computing*, vol. 24, pp. 210–223, 2015.
9. An Intelligent and Secure Health Monitoring Scheme Using IoT Sensor Based on Cloud Computing. -Jin-XinHu, Chin-LingChen, Chun-LongFan, and Kun-haoWang
10. Semantic Interoperability in Heterogeneous IoT Infrastructure for Health care.-Sohail Jabbar,

Farhan Ullah, Shehzad Khalid,
MuradKhan, and Kijun Han

Shanthashalini*, r. Shobana, s.
Leelavathy andV. Sridevi

11. Fog Computing-Based IoT for
Health Monitoring System Anand
Paul ,1 Hameed Pinjari,1 Won-
Hwa Hong ,2 Hyun CheolSeo
,2and Seungmin Rho 3

14. P. Tudor, W. Martin, B. Natalia, P.
Zeeshan, and B. Leon, “Ambient
Health Monitoring: the smartphone
as a body sensor network
component,” Innovation in
Medicine and Healthcare Inmed,
vol. 6, no. 1, pp. 62–65, 2013.

12. Secure Data Encryption for Cloud-
Based Human Care
ServicesTaehwan Park ,1
HwajeongSeo ,2 Sokjoon Lee,3
and Howon Kim 1

13. A CLOUD BASED APPROACH
FOR HEALTH
CAREMANAGEMENTK.

Cite this Article

Omkar Khot, Abhishek Basagare, Vahid
Mujawar, Jeenika Anadani, Rohini Mali,
Mahesh P. Gaikwad (2019) **Secure
Health Monitoring and Predictive
System Using Cloud Computing**
Journal of Data Mining and Knowledge
Engineering, 4(1) 30- 39

<http://doi.org/10.5281/zenodo.2641622>

AUTHORS' PROFILE

[1] OmkarKhot, Student

Department: Computer Science &Engineering

College: Sanjay Ghodawat Group of Institutions,Kolhapur, Maharashtra, India

[2] Abhishek Basagare, Student

Department: Computer Science &Engineering

College: Sanjay Ghodawat Group of Institutions,Kolhapur, Maharashtra, India

[3] VahidMujawar, Student

Department: Computer Science &Engineering

College: Sanjay Ghodawat Group of Institutions,Kolhapur, Maharashtra, India

[4] JeenikaAnadani, Student

Department: Computer Science &Engineering

College: Sanjay Ghodawat Group of Institutions, Kolhapur, Maharashtra, India

[5] Rohini Mali, Student

Department: Computer Science & Engineering

College: Sanjay Ghodawat Group of Institutions, Kolhapur, Maharashtra, India

Email Id: rohinimali321@gmail.com

[6] Mahesh P. Gaikwad, Assistant Professor

Department: Computer Science & Engineering

College: Sanjay Ghodawat Group of Institutions, Kolhapur, Maharashtra, India