ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

A Smart and Secure Architectural Model for IoT Based Health Care System

Prof. Vanitha T N[1], Akshitha G N[2], Deeksha K R[3], Hemavathi M U[4]

Assistant Professor, Department of Computer Science and Engineering, Sri Krishna Institute of Technology, Bangalore, India[1]

B.E Student, Department of Computer Science and Engineering, Sri Krishna Institute of Technology, Bangalore, India[234]

ABSTRACT: Among all applications enabled by the Internet of Things (IoT),smart and connected health care is a particularly important one. Networked sensors, either worn on the body or embedded in our living environments, make possible the gathering of rich information indicative of our physical and mental health. Farming is the foundation of India. Nowadays individuals in India losing the trust in cultivating the land because of the inclement weather. The agriculture joins its hands with technology to improve the productivity of agriculture. The improvements are in the selection of seed. The smart cultivating helps an awesome degree Agriculture Sustainability. Health care analysis is a data-rich domain. The Healthcare Internet of Things (HIoT) encompasses the new embedded sensing capabilities of devices together with the availability of always being connected, to improve patient care whilst reducing costs. Internet of Things(IoT) can be perceived as enabling user-specific interoperable communication services by integration of sensing and actuation technologies, with other leading technologies, such as telecommunication, networking,security, cloud computing etc. In this paper, we highlight the opportunities and challenges for IoT in realizing this vision of the future of health care.

KEYWORDS: Healthcare Internet of Things (HIoT) , IoT, Network Sensors

I. INTRODUCTION

Recent years have seen a rising interest in wearable sensors and today several devices are commercially available for personal health care, fitness, and activity awareness. In addition In healthcare big data refers to electronic health data sets which are so large and complex. A database is created that takes patient names and addresses from one system and matches it up with scheduled appointments from another system or integrating claims data with clinical notes from the EHR[Electronic Health Record]. Mending multiple sources of information together into a centralized databank accessed by reporting or a query system can provide a more in-depth and actionable snapshot of history of the patient, diagnoses, treatments, socio-economic challenges and other risk profiles. It is also used to envisage epidemics, cure disease, improve quality of life and avoid preventable deaths. Hospitals and healthcare systems are excellent depot of big data (like patient records, test reports, medical images etc.) that can be utilized to lower the cost in healthcare and to get better reliability and efficiency. The trend in healthcare is changing from cure to prevention. The examples of quantitative data are temperature, weight, age, total number of people suffering from the particular disease. Qualitative data consists of non-numerical data. The words can be used to portray the health related issues. The qualitative data cannot be measured, but can be observed. The examples of qualitative data are Female/Male, Non-smoker/Smoker etc. The term IoT defines the series of interconnected sensors, devices, and networks that monitor, collect and exchange information across real-time applications. The term IoT has two different aspects such as the network or the internet and things or objects. In recent years, IoT-based E-health applications acquire greater importance as it simplifies the complex healthcare management tasks into a refined process.

In addition to the technology for data gathering, storage and access, medical data analysis and visualization are critical components of remote health monitoring systems. Accurate diagnoses and monitoring of patient's medical condition relies on analysis of medical records containing various physio-logical characteristics over a long period of time.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Dealing with data of high dimensionality in both time and quantity makes data analysis task quite frustrating and error prone for clinicians. Although the use of data mining and visualization techniques had previously been addressed as a solution to the aforementioned challenge, these methods have only recently gained attention in remote health monitoring systems.The Healthcare Internet of Things (HIoT) is not just another wave of technology and consumer gadgets. The concept of Internet-connected devices, transferring data through the web, the cloud and traditional communication media, has seen the smart phone, mobile apps, and medical devices begin to converge. Many aspects of our lives are already impacted by this technology yet it is challenging industry, communications, health, economics, business models, IT, and security. Potentially, real time patient care will undergo a huge transformation with increased availability and the connectivity between sensors, medical devices, mobile technology, and clinical information systems

II. EXISTING SYSTEM

A context-aware framework for IoT-based E-Health system is given in [1]. It provides context-aware multimedia services to the E-Health users. This work gathers live user context from the sensor networks and heterogeneous internet based services. The major contribution of this work is to collect and analyze Electronic Health Records (EHR) from the sensor networks and to provide different services to the data users based on various contexts. A secure architecture framework for IoT-based E-Health security is given in [2]. It provides the necessary standards and privacy measures for the M2M and IoT-based E-Health systems. It states that authentication, authorization, encryption, decryption, auditing, access control and context based access are some of the building blocks of the secure IoT-based Ehealth systems. Also, it stresses the need for growing requirement to security and privacy measures across IoT-based E-Health systems. A comprehensive survey of IoT health care systems is given in [3].
It provides a collaborative security model to reduce the security issues across the health care systems. Also, it provides the impact of big data, ambient intelligence and wearable's across various E-Health contexts.It provides policies and regulations to improve IoT-based E-Health systems and define the set of challenges and research gap across the IoT-based E-Health systems. In [4] a state of the art of IoT techniques is given. It provides a complete description to significant technological drivers, potential applications, challenges and research gaps in IoT. Also, various perspectives and applications of the IoT systems are discussed in detail with its drawbacks and solution measures. The importance of security and privacy measures across IoT-based E-Health system is given in [5]. It states that privacy and security are the two primary constraints of the IoT-based health care systems. Also, suggests that data confidentiality, access control, enforcement of security and privacy policies across IoT devices and E-Health networks provides a better solution to the security and the privacy measures. It provides some of the existing research gaps across IoT-based E-Health systems and discusses the solutions available for it. Some of the open issues associated with the health care system are also given in this work. An integration of IoT and cloud computing systems are given in [6].
The technique of cloud computing can be merged together with the IoT applications in a variety of scenarios and it further provides effective solution. This work introduces a CloudIoT paradigm with its functionalities, underlying techniques and research issues. A detailed analysis of the cloud computing and IoT integration is given with it advantages and disadvantages. The analysis results states that the CloudIoT paradigm provides better system performance and security measures across various application especially with the healthcare systems. A federated IoT, and cloud computing based E-Health monitoring system is given in [7]. The widespread adoption of E-health systems enables the health service providers to continuously monitor the EHR's. This work states that scalability, flexibility, and energy efficiency are some of the drawbacks of the E-Health systems. To solve this issue, it introduces a pervasive patient health monitoring (PPHM) infrastructure. The PPHM architecture works by both the cloud computing and IoT technologies. It presents a cryptographic rolebased access control model for E-health systems. It makes use of user biometric identity for user authentication processes. It grants data access provision based upon the user biometric.

III. PROPOSED SYSTEM

A IoT- based E-Health Systems Architecture Elements: Architecture is one of the major design constraints across IoT-based E-Health systems. In general, we categorize the healthcare architecture into two types such as distributed and cloud-based architectures. We do not provide any information on centralized architecture because the EHR's are distributed in nature. It is distributed across multiple entities such as hospital, patients, doctors and research analysts for various purposes. This makes the application of centralized architecture inappropriate among IoT-based E-Health

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

systems. The distributed architecture consists of a set of servers connected together, and each has its own functionalities and appears as a single system. This type of architecture supports IoT-based E-Health systems as the EHR's are highly distributed in nature. In a distributed architecture a network of computer work together and achieves a common goal. This type of architecture is most suitable for clinical and hospital management systems. The patient health information's from the local hospitals are collected and stored across the distributed servers. The data stored on the distributed servers are then processed and analyzed for research and medication purposes through the central server. The drawback of this type of architecture is that it is not much suitable for real-time health monitoring systems. In a performance aspect, distributed architecture supports speed-up and lacks at scale up measures. Also, its performance degrades when dealing with huge amount of complex data. This due to the reason that it supports only the horizontal scaling and fails to deal with vertical scaleup.

Cloud based Architecture, In a cloud-based architecture there exists a trusted cloud service provider or a central authority (CA). It makes use of the public, private and hybrid cloud infrastructures. In a cloud-based architectures, the patient's health information's are monitored through the body area networks (BAN). The body sensors are projected in and around the patient's body through the wearable smart devices. The patient's health information's are monitored through the body sensors and sent to the cloud server for storage purposes. The patients can also track their health information's through the mobile devices. The Health service provider establishes the Service Level Agreement (SLA) with the patient's and manages EHR's across the cloud server. The cloud service provider (CSP) provides the health care services across the cloud computing environment. The CSP stores and manages EHR over the cloud computing infrastructure. Once the data is stored into the cloud server, the CSP imposes access policies and shares it with a trusted group of users. The user can gain access to the data only when the CSP defined access policy matches with the user data access policy. In general, there exist two different approaches such as patient-centric and non-patient centric approach. In a patientcentered approach, the patient's defines the access policies and shares the data. This approach becomes inefficient when dealing with emergency situations.

Thus the proposed system introduces the CSP centered approach, where the Cloud Service Provider (CSP) specifies the data access policies and acts as the entire responsibility for health data management processes. Also, the cloud-based architecture remains to be the most suitable solution for the IoT-based E-Health systems as it can handle large and complex EHR in an efficient manner. An verview of IoT-based E-Health System security .

IV. SYSTEM ARCHITECTURE

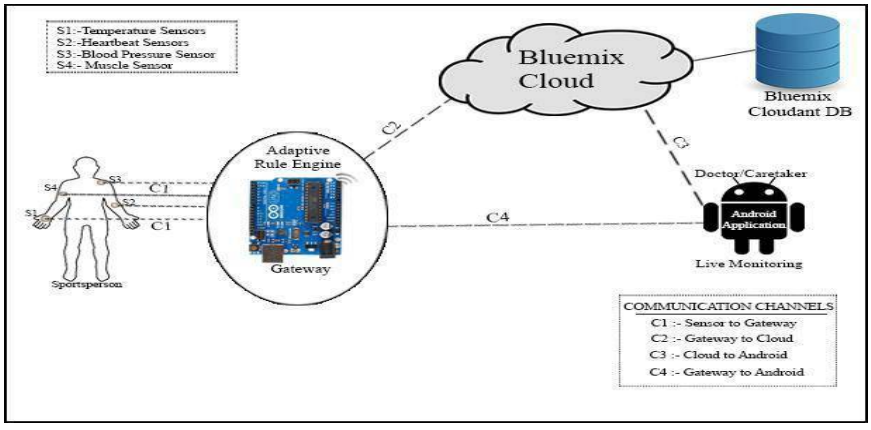

Fig. 1 System Architecture

In our system, we propose architecture (Fig. 1) which is based on a secure gateway which drives the entire system. The secure gateway is implemented here using Arduino MKRzero microcontroller board. To collect the body parameters of a sports person, we use temperature, heartbeat/pulse, muscle and blood pressure sensors. Sensors will collect the data and communicate with the gateway using a pre-shared key. This pre-shared key can be specified during the device configuration time itself. The gateway will then analyze the received data using an adaptive rule engine for any

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018
2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"
13th-14th March 2018
Organized by
Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

abnormalities in it. In case of any abnormalities detected, this will get notified to the monitoring device through a fast and secure channel which is enabled using a new key exchange scheme based on LEACH protocol. Gateway then transfers the data to cloud storage for future reference. The channel between the gateway and cloud is enabled using modified HIP-DEX protocol. End users (doctor/physio/any authorized person) can frequently monitor the health statistics of the sports person using an Android application. Communication between the end-user device and the cloud is again secured using modified HIP-DEX protocol.

V. SYSTEM IMPLEMENATION

To test the feasibility of the proposed architecture, we implemented it using four different sensors (Temperature, Pressure, Heartbeat and Muscle), ArduinoMKRZero board, IBM Bluemix cloud and an Android application. IoT system will be strong and efficient when it has been connected by both hardware and software via Internet. System communication will be highly secure by implementing lightweight key exchange scheme protocols. In this system, the data received from the device gets processed in the gateway before being stored in IBM Bluemix, which is a cloud environment. The results can be monitored by doctor or authorized caretakers through an Android application. An alert message will be send to the doctor or caretaker number if any critical situation occur. Through Live graph plot the variations in the data acquired will be monitored in Android application. Hardware part is more important in IoT systems, so this system consist of different sensors and these sensors have been connected to a microcontroller and we are using arduino as the controller.Gateway program in Arduino board: In our system, we propose an adaptive rule engine running in the gateway.

In this paper we have proposed a new protocol scheme based on LEACH routing protocol and the modified HIP-DEX key exchange scheme to secure the network communication in channels C1, C2, C3 and C4. HIP-DEX [9] is a lightweight key exchange scheme which provides better protection on DoS attack by using cryptographic puzzle mechanism. The primitives used in the algorithm are fixed and has no hash function included. It does not need more than 450 bytes for handshake transmission. In this work we use the little modified version of HIP-DEX which uses Elliptic Curve Qu-Vanstone (ECQV) implicit certificate instead of conventional ones to reduce the computational overhead. HIP-DEX cryptographic protocol is a two party protocol used to establish communication between hosts. The protocol is controlled by Initiator and Responder. It uses Elliptic Curve Diffie-Hellman keys for secrets session transmission. The working of HIP-DEX protocol is on the base of the packets used for transmission.The key exchange scheme used in this system is the modified HIP-DEX protocol is presented.In our implementation.

The Initiator I of the key exchange is the Gateway/Monitoring Device and Responder R is the cloud. In this scheme it have four packets. Initial packet, I1 initiates key exchange and rest of packets, R1, I2 and R2 point to the authentication of Master Key SA generation using Diffie-Hellman key exchange.The key exchange scheme protocol which we are proposed is based on LEACH routing protocol . Low Energy Adaptive Clustering In the proposed protocol we consider the energy efficiency of the sensors, sensors belongs to each group will transmit their energy

quality and MN will aggregate this information and transmit it to MD.The proposed scheme have three stages Initial authentication process, smart device registration and smart device key updating. Each state have different rules that to make the communication secure. This stages will control the network and send the data constantly in a secure channel.

ALGORITHM : Adaptive Rule Engine
InpuT:Data from sensors
Input:Health status
Initialisation: HardThreshold
Initialisation: SoftThreshold = HardThreshold
1: Generate
PR, QRS, QT interval
2: Compute
PR_interval Data
3: Compute
QRS_interval Data
4: Compute

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

QT_interval Data
5: Store the data in cloud database
6: Classify data is abnormal:
7: If Data > HardThreshold then :
8: Data may be abnormal
9: If Data > SoftThreshold then :
10: Check Data with each feature interval
11: If PR_interval.Data >= SoftThreshold.PR then :
12: PR_interval.Healthstatus
13: else if QRS_interval.Data >= SoftThreshold.QRS then :
14: QRS_interval.Healthstatus
15: else if QT_interval.Data >= SoftThreshold.QT then:
16:QT_interval.Healthstatus
17: end if
18: else
19: no change in SoftThreshold
20: end if
21 :else
22: Sportsperson Data is normal
23: end if

VI. EXPERIMENTS AND RESULTS

To evaluate the performance of our system we used MKRZero microcontroller powered by Atmel's SAMD21 MCU, support 32-bit ARM Cortex M0+core as the initiator (Gateway) and IBM Bluemix cloud environment as the responder. The adaptive rule engine running in the gateway will analyze the captured sensor readings and transfer the readings to Bluemix cloud. This communication is secured using modified HIP-DEX protocol. The java modules running in the initiator and the responder enables the communication process between them. The same protocol is used to secure the communication between cloud and the end-user device. We tested the performance of modified HIP-DEX protocol implementation by evaluating the processing time between the initiator and responder with different datasets.

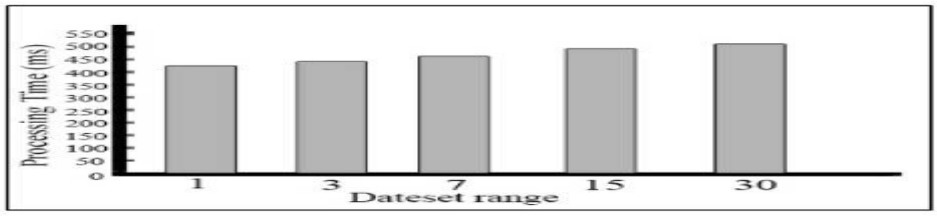

Fig. 3. Processing time of modified HIP-DEX protocol

Fig. 4. Android Application Screenshot

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

VII. CONCLUSION

In this paper, we reviewed the current state and projected future directions for integration of remote health monitoring technologies into the clinical practice of medicine. Wearable sensors, particularly those equipped with IoT intelligence, offer attractive options for enabling observation and recording of data in home and work environments.
Smart and secure healthcare systems which monitor the health condition of a person and inform any abnormalities to doctor or caretaker will definitely help the person to maintain his fitness to a certain extent. In this study, we have proposed a very efficient and secure architectural model for IoT based healthcare systems. Advancement of IoT technologies have made the implementation of such a system possible.

REFERENCES

[1] I. Nikolaevisjiy, D. Korzun and A. Gurtov, "Security for Medical Sensor Networks in Mobile Health Systems," IEEE Int. Symposium on a World of Wireless, Mobile and Multimedia Networks 2014.
[2] M. F. A. Rasid et al., "Embedded gateway services for Internet of Things applications in ubiquitous healthcare," 2014 2Int. Conf. Commun Technol. ICoICT 2014, pp. 145-148, 2014.
[3] P. P. Ray, "Internet of Things for Sports (IoTSport): An architectural framework for sports and recreational activity," Int. Conf. Electr. Electron Signals, Commu Optim EESCO 2015.
[4] M. Umer, B. A. Bhatti, M. H. Tariq, M. Zia-ul-hassan, M. Y. Khan, and T. Zaid, "Electrocardiogram Feature Extraction and Pattern Recognition Using a Novel Windowing Algorithm," no. October, pp. 886-894, 2014
[5] I. Value and E. Team, "Sports Analytics and Risk monitoring based on Hanna Platform," ISOCC 2015 pp. 221- 222, 2015
[6] X. M. Zhang and N. Zhang, "An open, secure and flexible platform based on internet of things and cloud computing for ambient aiding living and telemedicine," 2011 Int. Conf. Comput. Manag. CAMAN 2011, pp. 1- 4, 2011
[7] R. Moskowitz. HIP Diet Exchange (DEX): draft-moskowitz-hip-dex-00, Aug. 2012. Standards Track no.C, pp. 1-39, 2013
[8] M. P. R. S. Kiran, P. Rajalakshmi, K. Bharadwaj and A. Acharyya, "Adaptive rule engine based IoT enable remote health care data acquisition and smart transmission system," 2014 IEEE World Forum Interne Things, WF-IoT 2014, pp.253-258, 2014