Industrial Engineering Journal
ISSN: 0970-2555
Volume : 49, Issue 7, No. 1, July : 2020

DESIGNING AND DEVELOPMENT OF SECURED ARCHITECTURE IN SMART HEALTH CARE SYSTEMS USING THE INTERNET OF THINGS

V. Kusuma Priya, P. Nagendra Babu, G. Muni Nagamani, Dept of Computer Science and Engineering, Sree Venkateswara College Of Engineering, Nellore (Dt), Andhra Pradesh, India.
P.Ravi Kumar, Dept of Electronics and Communication Engineering, Sree Venkateswara College Of Engineering, Nellore (Dt), Andhra Pradesh, India.

ABSTRACT
In fact, the conventional healthcare systems were servile. Even for mild difficulties, the patient had to see the doctor frequently. The IoT has made the dream of a smarter world a reality and has a wide range of applications, including healthcare. This problem has been resolved with the development of intelligent healthcare systems, which has decreased death rates globally. The adoption of Healthcare IoT might improve the lives of patients as well as the standard of care given by doctors, nurses, clinicians, pharmaceutical firms, and the general public. This article discusses the Design and Implementation of Secured Architecture for Smart Health Care System Using Internet of Things. This intelligent healthcare model is evaluated in the MATLAB environment to overcome packet loss and other problems. This study looks at the Cloud Request View Ratio (CRVR), packet loss, and success rate of the Internet of Things as it now exists in the healthcare system. Then, advocates for security and privacy solutions discuss difficulties in implementing security frameworks.

Keywords: IoT, Security, Smart health systems, privacy

1. INTRODUCTION
A wide range of online services are now available thanks to the quick advancement of digital processing technology and excellent networking. In order to ensure the viability of human social contact, these services leverage the Internet of objects (IoT) as a conduit linking people, objects, and processes [1]. Thanks to these web-based service-based technologies, research is shifting from centralised to decentralised environments. IoT has made great progress in the digital era thanks to a wide range of possible applications, such as smart agriculture, smart health care, smart traffic management, and others [2]. The Internet of Things (IoT) integration has increased productivity, reduced costs, and created insightful data, all of which have improved quality of life in different ways. In order to improve patient monitoring, reduce expenses, and foster innovation in patient care, IoT is being utilised in healthcare.
New techniques for remote monitoring, autonomous assistive solutions, pharmaceutical administration, early warning and proactive treatment programmes, asset management, and equipment maintenance have been made feasible as a result. An interconnected system of physical objects and sensors known as the Internet of Things (IoT) allows for data collection, computation, analysis, and decision-making. For business and a number of socially relevant operations, the use of data exchange to link and interact between IoT devices and objects and the environment is essential [3]. The idea of the Internet of Things has changed the focus of communication from being between people to being between things or between things and people.It is essentially a platform for a variety of similar or dissimilar objects with unique identifiers that are used in conjunction with sensors, electronics, and network connectivity to help these things and objects gather, process, and transfer data in order to bring to life the scenario of device-to-device or person-to-machine communication. It makes it possible for people and devices to

connect at any time, anywhere, and everywhere. Therefore, it becomes crucial to understand how communication works in the IoT domain.For patients' safety, efficient care, and privacy protection, security and privacy protections for Healthcare IoT devices are essential.On the other hand, the medical industry is where the bulk of security lapses and data privacy problems are disclosed [4]. Malware, human interference for financial gain, and the theft of personal sensitive medical data for use by other parties pose a serious threat to medical data. Surprisingly, many of the state-of-the-art IoT solutions now available do not give security and privacy structures the attention and effort that they need. Due to these serious security flaws, sensitive personal data privacy issues arise. One of the key IoT application areas is smart healthcare. Academics and academics have been focusing increasingly on this area in recent years to address the potential of the IoT in the healthcare industry [5]. There are several services, apps, and prototypes in the field that take into account the many practical issues. Network architectures and associated platforms, interoperability, heterogeneity, security, new services, and applications are all topics of IoT-based Smart Healthcare research. For the purpose of developing IoT technology in the healthcare industry, guidelines and policies have been framed. Despite all of these efforts, IoT in the healthcare industry is still in its infancy. The piece is set up as follows: The work is ended with Section V, which follows Section II's explanation of the literature review and Section III's description of the methodology.

2. Review of Literature

U. Satija, B. Ramkumar, M. S. Manikandan, et al.'s study [6] showed a stronger contribution to the use of wearable sensors and smartphones for health monitoring, particularly in emergency notification and detection with adequate life-saving benefits in distant regions with limited bandwidth. Additionally, they address the requirement that international patients be given top priority in healthcare systems due to the inadequacy of the capacity to deliver timely medical care to each patient. It is unbearable to people who come from other areas that specially trained physicians and nurses give priority to patients who physically arrive at the emergency department. Prioritising patients via telemedicine before transferring them to hospitals is deemed to be a practical tactic.

The function of IoT in healthcare delivery was outlined by Sapna Tyagi, Amit Agrawal, Piyush Maheswari, et al. [7], who also looked at the prospects and the technology components that made it possible. This system creates a network connecting all healthcare-related entities (doctors, patients, labs, chemists, nurses, etc.) that extends beyond those located in a single geographic region. tried to put into practise the IoT notions where these things would be talking to the cloud directly.

Mikael.A and S. Nadjm-Tehrani, et al. [8] have investigated the need for security in systems that control important social services including electricity, water, and health. The writers have discussed the security challenges associated with IoT implementation. According to some, the major issue on the device side is that IoT or M2M/IoT devices lack the capabilities to do encryption on the device. It is suggested to build memory-efficient representations and a CPU-efficient method in real time to allow lightweight intrusion detection.

Nicolae Botezatu, Elena Serban, Paul Corneliu Herghelegiu, Andrei Zal, et al. [9] outlined the steps taken to design and build a low-cost monitoring system prototype. The method concentrates on monitoring patients remotely in hospital wards following an ICU discharge. The device provides mobile support and allows for faster and more effective medical care in situations of emergency by using low-power, specially developed sensor arrays for temperatures and mobility.

S. M. Raizul Islam, Daehan Kwak, MD, Humaun Kabir, and Kyung-Sup Kwag, et al. [10] talked about the ways in which cutting-edge technologies, like big data, surrounding intelligence, and wearables, are

used in a healthcare context. Someone additionally addressed various IoT and eHealth and laws within the world. Described the developments in IoT-based health care technology as well as examined the special privacy and security aspects, security needs, threat models, and attack taxonomy within a health care approach.

Internet of Things-Based Smart Health Care System

Architecture of Design and Implementation of Secured Architecture for Smart Health Care System Using Internet of Things is represented in below Fig. 1.

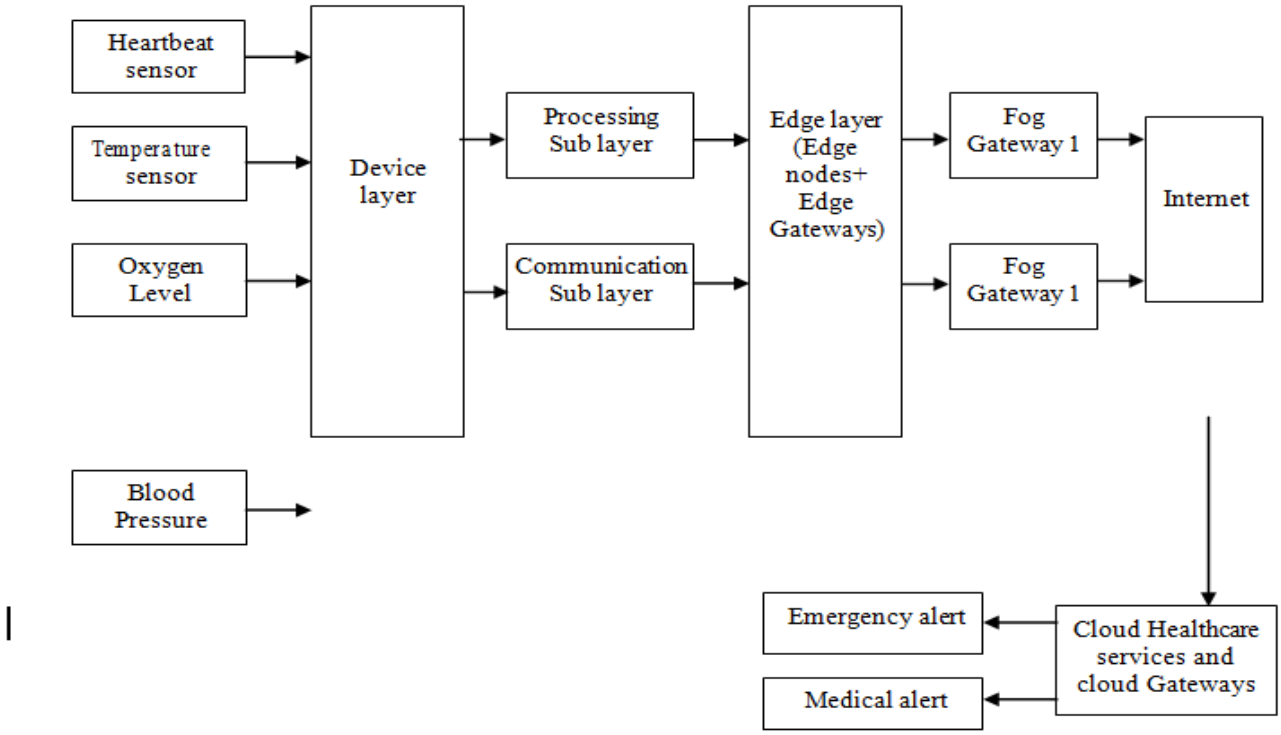

Fig.1: System Architecture for proposed model

IoT dramatically improves the standard of healthcare goods, services, and patient-centered, individualised therapies. The smart health environment is another element from which the patients' unprocessed data are obtained for use in subsequent data aggregation and analysis procedures. The majority of patient-focused technology is equipped with sensors or microchips. The human body, or the body of the patient, is connected to the numerous health sensor equipment. The sensors can measure things like blood pressure, temperature, oxygen levels, and heartbeat.

In order to transport healthcare data to gateways utilising Bluetooth, Zigbee, and WiFi, sensors and smart medical devices combine cloud-based services with edge or node computing. The processing layer of wide-area communication technologies like 4G LTE, LoRaWAN, and NB-IoT then transports this to the data centre. In order to collect contextualised personal medical data for each patient, physical equipment such as portable, implantable, and other tracking devices are linked to a tiny wireless module in the device layer.

This enormous amount of data is processed and analysed by the data centre before being shared with each patient in detail. The gateway is responsible for giving messages a conduit, enabling communication across many platforms, and enabling various services including data processing,

publishing, and subscribing the data generated by various sensors. The main function of this layer is calculation. However, the majority of the data can be preprocessed on mobile devices by making use of the available resources. consists of fog layer networked smart gates.
This layer enables the IoT network to support a local repository for connected subnetworks and provide intelligence to edge nodes. Data from a subnetwork is gathered by smart gateways, which also change protocols and provide more sophisticated services. Smart health gateways safely and effectively manage remote end-user authentication and authorization on behalf of medical sensors. Mutual authentication between the medical device and the smart gateway is required during startup. Data warehouses, big data analysis servers, a remote healthcare server that regularly syncs with the hospital database, and other components make up the final cloud layer. The processed data from the previous layer is maintained at this layer for analytics, decision-making, and other applications.
This data is used to learn and identify trends that will improve patient care and welfare, in addition to being used to gather information on a patient's medical history and current state of health. After the user or patient has been verified, the notifications are sent to the Smart Gateway by the Information Alert Server. Once authentication is complete, the needy are given coded health notifications. Emergency and medical notifications are sent to ambulances and the appropriate medical personnel using location-based data and the Data Management Server. Health service providers are duly certified and permitted to deliver certain services. Therefore, the IoT-enabled smart health service is totally secure. The health metrics of the IoT client are kept private by demanding user identity.

2. RESULT ANALYSIS

This smart healthcare model was put into action using the MATLAB R2016a programme, which runs on a computer with an Intel Core I5 processor clocked at 2.27 GHz, 8 GB of RAM, and Windows 8 OS. The outcomes of this model are evaluated in comparison to popular methods focused on healthcare applications.Table 1 presents the performance analysis in comparison to the conventional healthcare system. For the performance analysis, a total of 1000 service requests or service hits were taken into account. The success percentage is 99.8%, which is a better outcome than the 0.2% packet drops that were observed. While the traditional healthcare system has a success rate of 94.4% and a packet drop rate of 5.6%.

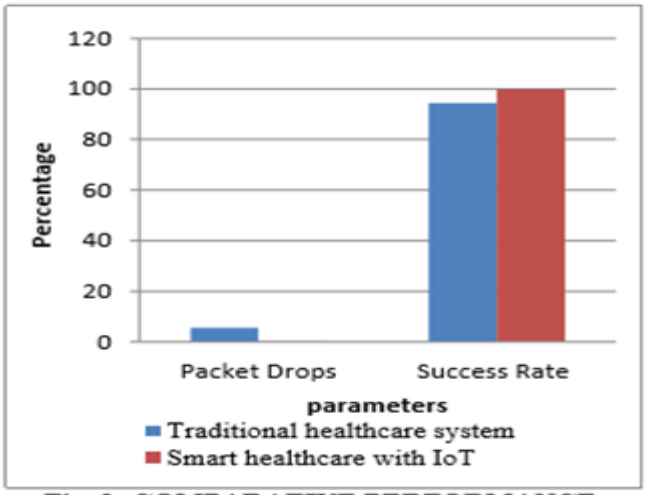

Fig.2: Comparative Performance

Both traditional healthcare systems and smart healthcare with IoT are analysed using cloud request

view ratio (CRVR) values, and it has been shown that traditional healthcare systems have a clear view of all unnecessary requests, even if CRVR is lower for this model. The important finding highlights the use of cloud consensus. This model, which now has a lower CRVR, handles the accessible view of the EMR (Electronic Medical Record). This lower CRVR is thought to be advantageous for privacy concerns.

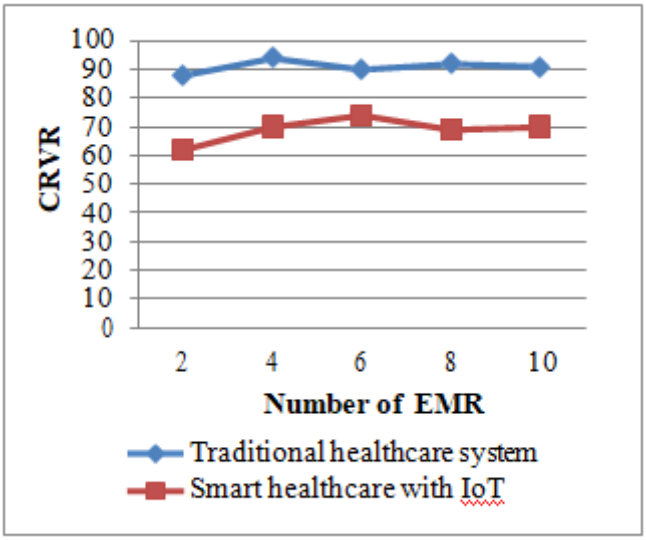

Fig.3:CRVR COMPUTATION

Therefore from results it is clear that patient data is secured with high privacy. Whenever the data is retrieved from cloud then the process of retrieving the EMR s are very fast and accurate. On the other hand, data from sensors are not normal then emergency alert send to the doctor or relates.

CONCLUSION

The design and implementation of a secure architecture for a smart healthcare system that makes use of the internet of things are covered in this article. Given the sensitivity of healthcare data, it is crucial to explore how to create smarter apps in a secure manner. This smart healthcare model was evaluated in a MATLAB environment to handle packet loss and success rate. A better result is that the success rate is 99.8% and the packet drops are only 0.2%. This lower CRVR is thought to be advantageous for privacy concerns. In the event that sensor data is abnormal, a doctor or related party will receive an emergency alert. Therefore, it is evident from the results that patient data is protected with high privacy.

REFERENCES

1. Nurassyl Zholdas,Octavian Postolache,MadinaMansurova,"Health MonitoringSystemUsing Internet of Things",2021IEEEInternationalConferenceonSmartInformationSystemsandTechnologies(SIST), Year: 2021
2. ObaidullaAl-Mahmud,KausarKhan,RajdeepRoy,FakirMashuqueAlamgir,"Internet of Things (IoT) BasedSmart Health Care Medical Box for ElderlyPeople", 2020 International Conference forEmergingTechnology(INCET), Year: 2020
3. AlokKumarGupta,RahulJohari,"IOT basedElectrical Device Surveillanceand Control System", 2019 4th InternationalConferenceonInternetofThings:SmartInnovationandUsages(IoT-SIU),Year:2019

4. Inderpreet Singh,Deepak Kumar,SunilKumarKhatri,"ImprovingTheEfficiencyofE-Healthcare System BasedonCloud",2019AmityInternationalConferenceonArtificial Intelligence(AICAI),Year:2019
5. Akshat,Gaurav,Zahid,Bhupendra,Aditi,SachinKumar,Maneesha,PraveenPandey,"A Smart Healthcare MonitoringSystemUsingSmartphoneInterface",
20184thInternationalConferenceonDevices,CircuitsandSystems(ICDCS), Year:2018
6. U.Satija,B.Ramkumar,andM.S.Manikandan,"Real-timesignalquality-awareecgtelemetrysystemforiot-basedhealthcaremonitoring,"IEEEInternetofThings Journal, vol. 4, no. 3, pp. 815-823,2017.
7. SapnaTyagi,AmitAgrawal,PiyushMaheswari,"AConceptualframeworkforIoT-based Health care System using CloudComputing",SixthInternationalConference CloudSystemandBigDataEngineering,July2016, pp. 503-507.
8. Mikael.AandS.Nadjm-Tehrani,"AttitudesandPerceptionsofIoTSecurityinCriticalSocietalServices,"inIEEEAccess,vol.4,pp.2130-2138,doi:10.1109/ACCESS.2016.2560919,2016
9. AlexandruArchip,NicolaeBotezatu,Elena Serban, PaulCorneliu Herghelegiu andAndreiZal,"AnIoTBasedSystemforRemotePatientMonitoring",SenenteenthInternational Carpathian ControlConference,June2016, pp.1-6.
10. S.M.RaizulIslam,DaehanKwak,MD. Humaun Kabir, Mahmud Hossain andKyung-Sup Kwag, "The Internet of Thingsfor Health Care: A Comprehensive Survey",IEEEAccess,vol.3,pp.678-708,April2015