A SECURED ARCHITECTURE FOR IOT-BASED HEALTHCARE SYSTEM

Palak Barapatre
B.Tech Student, Department of Electronics and Communication Shri Ramdeobaba College of Engineering and Management Nagpur, (India).
E-mail: barapatrepv@rknec.edu

Yash Ingolikar
B.Tech Student, Department of Electronics and Communication Shri Ramdeobaba College of Engineering and Management Nagpur, (India).
E-mail: ingolikaryj@rknec.edu

Prajakta Desai
B.Tech Student, Department of Electronics and Communication Shri Ramdeobaba College of Engineering and Management Nagpur, (India).
E-mail: desaipm@rknec.edu

Pooja Jajoo
B.Tech Student, Department of Electronics and Communication Shri Ramdeobaba College of Engineering and Management Nagpur, (India).
E-mail: jajoopd@rknec.edu

Prasheel Thakre
Assistant Professor, Department of Electronics and Communication Shri Ramdeobaba College of Engineering and Management Nagpur, (India).
E-mail: thakrepn2@rknec.edu

Reception: 11/11/2022 **Acceptance**: 26/11/2022 **Publication**: 29/12/2022

Suggested citation:

Palak Barapatre, Yash Ingolikar, Prajakta Desai, Pooja Jajoo, and Prasheel Thakre. (2022). A secured architecture for IoT-based healthcare system. *3C Empresa. Investigación y pensamiento crítico, 11*(2), 222-230. https://doi.org/10.17993/3cemp.2022.110250.222-230

https://doi.org/10.17993/3cemp.2022.110250.222-230

ABSTRACT

Healthcare has gradually moved away from the model centered on traditional health centers due to the emergence of highly accurate sensors and Internet of Things (IoT) enabled medical equipment. Ambient intelligence takes whatever actions are required in response to a recognized event in order to enable continuous learning about patient data. The capabilities of IoT-assisted healthcare services might be improved by incorporating autonomous control and human-computer interface (HCI) technologies into ambient intelligence. Major unsolved issues include the privacy and security of information collected by medical IoT devices, both during transmission to and during cloud storage. This research explores different techniques, IoT factors, and features, with an emphasis on the data security concerns connected to data flow in medical IoT. In order to guarantee data security and privacy at all data levels, this study suggests a safe design for the IoT healthcare system.

KEYWORDS

HealthCare, Internet of Things, Secure IoT Networks, Privacy and Security HCI, Cloud Computing.

https://doi.org/10.17993/3cemp.2022.110250.222-230

1. INTRODUCTION

The Internet of Things principal objective is to connect every device on the earth. Today, IoT is mostly employed in healthcare to provide instant access to information. The IoT is a network of autonomous computing devices, mechanical and digital machines, animals, or humans. It connects everything to the Internet, encourages information exchange, organizes correspondence, and enables item positioning, tracking, administration, and monitoring. It provides information technology (IT) solutions, which employ computers to store, retrieve, transfer, and modify data without requiring human-to-human or human-to-computer interaction. According to its definition, the Internet of Items (IoT) is a "dynamic worldwide interconnected network technology with self-configuring capabilities based on standard and coherent communication protocols where virtual and physical things have identities, physical characteristics, and virtual personalities". Integrating a number of promising technologies will enable the IoT idea to be realized in the real world Jeong et al. [2016] Darshan et al. [2015] Thakre et al. [2022]. IoT may be combined with identification, sensing, and communication technologies. Security concerns, in addition to heterogeneity, scalability, connection, and many other problems, are significant hindrances to the growth of the Internet of Things and must be adequately addressed if IoT is to be successful. Among other security challenges like confidentiality, integrity, etc., authentication of devices participating in the IoT is one of the more significant ones and is the main theme of this article. IoT development has now been supported by a variety of technologies, including NOMA in wireless technology, MEMS, and the Internet Thakre et al. [2022] Kinhikar, et al. [2022]. A market worth more than 2.1 trillion dollars is predicted to emerge by 2025 owing to the low cost of sensor devices, resulting in more than 25 billion installed units by 2020. A market worth more than 2.1 trillion dollars is predicted to emerge by 2025 owing to the low cost of sensor devices, resulting in more than 25 billion installed units by 2020.

2. RELATED WORK

2.1 ARCHITECTURES

In the context of the IoT, the authors Almotiri et al. [2016] presented a mobile health (m-health) system (IoT). The use of mobile devices to obtain real-time health information from patients and store it on network servers connected to the Internet is known as m-Health.

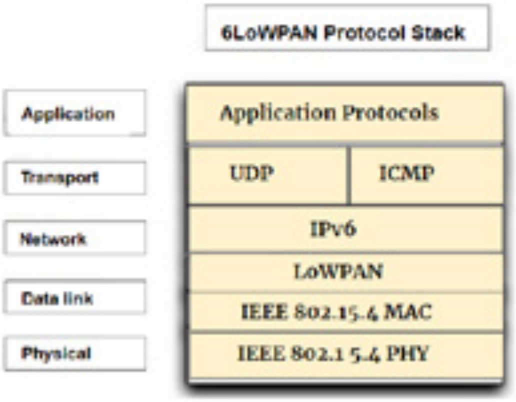

Fig 2.1: Protocol Stack.

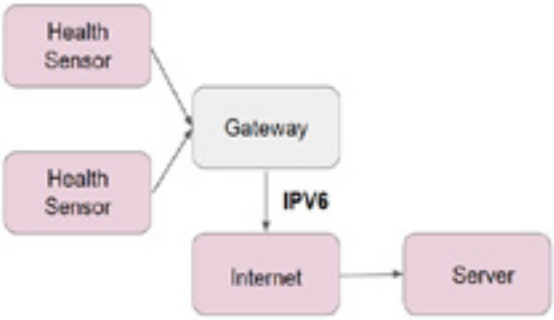

Fig 2.2: Related Architecture.

https://doi.org/10.17993/3cemp.2022.110250.222-230

In real-time, intelligence algorithms evaluate m-health data to find trends and raise different alarm levels based on the status of the observed patients. An m-health system's information technology architecture is a component of the IoT architecture, which is multi-layered and includes data collection, data storage, and data processing layers. In , T. N. Gia et al. [2014] the 6LoWPAN architecture, which is composed of low-power wireless area networks (LoWPANs)2, which are IPv6 stub networks for IoT networks, is described. 6LoWPAN has emerged as the favored option. Sensor nodes employ the 6LoWPAN protocol stack, represented in Figure 2, to transmit data to the network. The sensor data is encapsulated in a 6LoWPAN datagram and delivered over an IEEE 802.15.4 frame to the edge router or gateway. The packets are converted to IPV6 packets by the gateway and sent to the server for additional data processing through the standard IPV6 network. In Fig 2 depicts the end-to-end architectural features of the 6LOWPAN-based healthcare system.

2.2. SECURITY ENCURITY MODELS

Privacy protection has been widely researched and accepted as a bottleneck in smart medical healthcare. Goldwasser and Micali introduced a GM encryption system that proved semantic security under the assumption of quadratic residuosity (Shafi & Silvio, 1984).The ideal lattice-based encryption scheme proposed by Gentry [2009] was the first response to all encryption-related problems up to 2009 Cheon & Kim [2015]. A method to significantly boost totally homomorphic encryption's efficacy was put out by Chen, Ben, & Huang [2014]. In Cheon & Kim [2015] suggested sacrificing additional public keys in favor of lowering the exponentiation circuit's degree. In Ichibane et al. [2014] explained how to choose encryption parameters in several real-world settings.

3. PROPOSED ARCHITECTURE FOR IOT-BASED HEALTHCARE SYSTEM

The system under the proposed design uses IoT sensors to gather patient data, which is subsequently sent to the hospital's cloud storage. Five parts make up the architecture.

3.1. IOT DEVICES IDENTIFIED FOR MEASUREMENT ARE

Blood glucose sensor: An opto-physiological glucose sensor, which measures blood glucose levels using a photodiode and an accelerometer, can be utilized in a non-invasive IoT system for glucose monitoring.

Temperature monitoring sensor: A Raspberry Pi-based temperature monitoring system and a planned wireless network of sensors would alert a doctor if a patient's temperature rose over a certain level. The LM35 sensor is proposed as a device for sensing the body's core temperature.

Healthcare systems for the elderly: An approach for detecting falls among the elderly and informing concerned parties is described. The system detects falls using sensor values from the accelerometer and gyroscope. These should be simple for the monitoring systems to dismiss as false positives and not register as falls. The waist is the right location to implant the sensors to detect geriatric falls, according to an examination of diverse sensor implantation sites on the body using various types of sensors and algorithms for machine learning.

Electrocardiogram heart monitoring systems: A minimal-cost ECG system is recommended. The ECG sensor in this system is merely a data collection device. Multiple users' ECG values are collected with the ECG sensor and sent via Zigbee to a centralized server.

Heart Rate Monitoring: Instant heart rate monitoring is a feature of several popular models, including Fitbit and Garmin as reviewed in Kumar N. [2017]

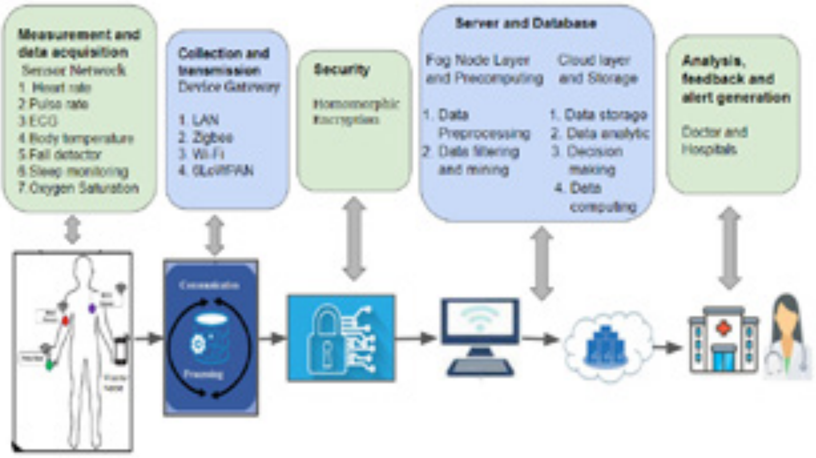

Fig 3.1: Proposed Architecture.

3.1.1. SENSORS IN IOT-BASED HEALTHCARE SYSTEMS

A minimal cost ECG system is recommended. The ECG sensor in this system is merely a data collection device. Multiple users' ECG values are collected with the ECG sensor and sent via Zigbee to a centralized server. The MMA7260QT accelerometer is specifically suggested for use in detecting body movement. Angular velocity can be measured along the x, y, and z axes using a device with three axes. A gyroscope can help alert medical workers when a person falls by detecting body tilt. A magnetometer aids in determining the relative direction by measuring the magnetic field. A magnetometer can detect a human fall when combined with an accelerometer, gyroscope, and other sensors, and is frequently seen in aged care equipment. Applications used: Raspberry Pi: According to, body temperature monitoring devices are created using the Raspberry Pi platform. A multispectral system that monitors body temperature, respiration rate, heart rate, and movement is developed using a Raspberry Pi as reviewed in Kumar N. [2017].

3.2. COLLECTION AND TRANSMISSION

Sensors are fastened to the patient's body to collect and transmit data to the master node in real time. The data from the master node is received by the mediator device and sent to the cloud. The collection and storage of data in the cloud is an ongoing process. The IoT sensors based on WiFi and Zigbee have the lowest latency, as shown in Table 3.2. Material is delivered to hospital servers using gateway nodes installed in the area for the protocol conversion from ZigBee to TCP/IP.

Table I. Comparison of available wireless communication technologies for smart healthcare.

Technology	Frequency	Types	Power usage	Range	Rate of Data
NFC	13.56 MHz	PAN	Very low	10 cm	100-400kbps
Bluetooth 4	2.4 GHz	PAN	Low	0.1km	1Mbps
Bluetooth 5	2.4 GHz	PAN	Very low	0.25 km	2Mbps
Z-wave Alliance	900 MHz	LAN	Very low	30m	9.6/40/100 kbps
Wi-Fi	2.4 GHz and 5GHz	LAN	Low-High	50 m	1Gbps
Zigbee	2.4GHz	LAN	Very low	10-100 m	250kbps

https://doi.org/10.17993/3cemp.2022.110250.222-230

Low-power sensor nodes can now be connected to the internet utilizing the Internet protocol, owing to communication protocols like 6LoWPAN. In order to function, the IPV6 protocol needs a substantial amount of computing power and bandwidth. They foresee "always-on" activity, which IoT devices do not. The study Ge et al. [2016] discovered that delivering these signals as JSON packets rather than XML packets significantly reduces response, processing, and interpretation times.

3.3. COMPUTING AND SECURITY

In fog computing, fog nodes (which can be access points, switchers, gateways, routers, etc.) are spread at the network's edge and move toward terminal facilities at a certain location. The fog computing layer is composed of the security, storage, and monitoring layers. Fog computing converts cloud data centers into uniformly spread platforms while aiming to sustain cloud services. As a result, there is a decrease in processing time for data from wireless medical sensors, which improves customer satisfaction and service level. Because storage nodes are low and also have limited power capacity, the public key encryption method cannot be employed for security. The research defines fog computing as the addition of cloud computing to the system's edge, which is a highly virtualized stage of the source pool that delivers computation, storage, and networking resources to local end users. The results indicate that fog computing may achieve more than 89% low latency and bandwidth efficiency. Because the fog nodule has a specified limited size, it cannot contain a large number of activities each second Yi et al. [2014], Kumar Y. et al. [2019]. Fog computing in health care was the focus of Isa et al. [2020]. In this study, a heart monitoring application was developed in which each patient was required to provide a 30-minute recording of their electrocardiogram signal to fog processing units for handling, analysis, and decision-making. The values are decreased so that less energy is utilized in both processors and networking equipment. When compared to the central cloud, the results show that energy may be saved by up to 69%.

To keep information confidential and private, it is necessary to encrypt it before it is delivered across a public channel and stored on fog nodes or cloud servers. After receiving information and instructions from the user and the cloud, they are responsible for filtering the raw data and uploading it to the cloud for long-term storage or additional analysis.

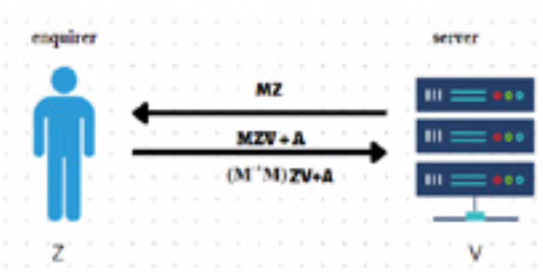

Fig 3.3: Homomorphic encryption.

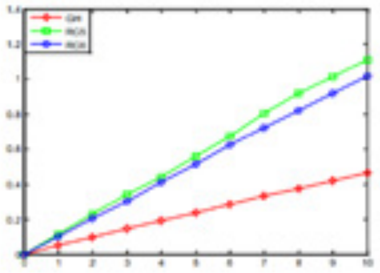

Fig 3.4: Comparison between different encryption models.

Steps for Homomorphic encryption

Step 1: The inquirer describes the data collected as a vector Z = (z1,z2,z3,.....,z8). After that, the secret eight-order invertible matrix M is generated. MZ is then computed and sent to the server.

Step 2: On the server, an intermediate vector V represented by V = (v1,v2,v3....v8) is stored. The greatest (denoted as Mx) and smallest (denoted as Mn) values of each physiological item's normal zone are likewise kept, and Li = Mx - Mn is discovered, with xi set to be 1/Li. In addition, we create matrix A, the elements that form the leading diagonal are equal to Mid, where Mid= -Mn/Li.

https://doi.org/10.17993/3cemp.2022.110250.222-230

Step 3: When the medical result MZ arrives at the server, it is multiplied by V to get MZV. MZV and matrix A are then returned to the enquirer by the server. The enquirer then obtains ZV by left multiplying it by M-1. Finally, Di is obtained by multiplying matrix A by ZV.

Step 4: If Di is in the range [0, 1], the data item remains normal. If Di is more than one, the data item appears too high; otherwise, it displays too low.

Even if the attackers are capable of stealing data passing through the communications platform, such as MZ and A, the data vector Z is left multiplied by M. If the proposed homomorphic encryption mechanism is used, hackers will be unable to access genuine data because they do not know M.

Fig (3.4) shows that the proposed encryption algorithm outperforms RC5 and RC6 in terms of efficiency. Several experiments were carried out to demonstrate its speed.

3.4. ANALYSIS OF DATA

Following the acquisition, the acquired data must be handled, filtered, and compressed to eliminate extraneous information. We can use the ontology technique, as proposed in the article Kumar V. [2015]. Clinic data for patients is specified as a source with a specific URL address in the recommended approach. To enable information transmission via Ontology data access, mapping with both previously collected and newly acquired records should be carried out after the acquisition of patient records. The doctor will create a treatment strategy for the patient after considering these variables, which will include the drugs and dosages that will be used. In this instance, the relationship is represented by the Protégé tool. Run a sparql query to get data or an owl/rdf file from the database.

4. CONCLUSION

This paper provides an in-depth examination of the most recent advancements in the IoT-based healthcare ecosystem, as well as a framework for IoT healthcare, a smart healthcare system, and its logical architecture. Sensors in a smart healthcare system collect medical information, data is collected via mobile and smart networks, data is transferred to cloud computing for analysis with advanced algorithms, and medical professionals can make treatment and diagnosis recommendations. The implementation of the IoT based healthcare system is split up into three features, with details on each presented. A homomorphic strategy based on a scrambling matrix was developed to address current problems of security in the IoT field. With the rapid development of IoT, we can anticipate that our medical healthcare system will have a wide range of applications.

REFERENCES

[1] Kinhikar, M., Agrawal, A., Tiwari, D., Kohad, I., Thakre, P., & Pokle, S. (2022). Outage Probability and Capacity Analysis for NOMA based 5G and B5G Cellular Communication. International Journal of Next-Generation Computing, 13(5).

[2] Chen, L., Ben, H., & Huang, J. (2014). An Encryption Depth Optimization Scheme for Fully Homomorphic Encryption. International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI), , (pp. 137-141).

[3] Cheon, J. H., & Kim, J. (2015). A Hybrid Scheme of Public-Key Encryption and Somewhat Homomorphic Encryption. IEEE Transactions on Information Forensics and Security, 1052-1063.

[4] Darshan, K. R., & Anandakumar, K. R. (2015, December). A comprehensive review on usage of Internet of Things (IoT) in healthcare system. International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT) (pp. 132-136). IEEE., 132-136. http://doi.org/10.1109/ERECT.2015.7499001

[5] Ge, S. Y., Chun, S. M., Kim, H. S., & Park, J. T. (2016). Design and implementation of an interoperable IoT healthcare system based on international standards. 13th IEEE annual consumer communications & networking conference (CCNC), (pp. 119-124).

[6] Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. IEEE, 169-178.

[7] Ichibane, Y., Gahi, Y., Guennoun, Z., & Guennoun, M. (2014). Private Video Streaming Service Using Leveled Somewhat Homomorphic Encryption. Tenth International Conference on Signal-Image Technology and Internet-Based Systems (SITIS), (pp. 209-214).

[8] Isa, I. S., El-Gorashi, T. E., Musa, M. O., & Elmirghan, J. M. (2020). Energy Efficient Fog-Based Healthcare Monitoring Infrastructure. IEEE Access, 197828-197852.

[9] Jeong, J.-S., Han, O., & You, Y.-Y. (2016). A design characteristic of smart healthcare systems as the IoT application. Indian Journal of Science and Technology, 9(37), 52, 9(37), 1-8. doi:10.17485/ijst/2016/v9i37/102547

[10] Kumar, N. (2017). IoT architecture and system design for healthcare systems. International Conference on Smart Technologies for Smart Nation (SmartTechCon), (pp. 1118-1123).

[11] Kumar, V. (2015). Ontology based public healthcare system in internet of things (IoT). 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15), (pp. 99-102).

[12] Kumar, Y., & Mahajan, M.. (2019). Intelligent Behavior Of Fog Computing With IOT For Healthcare System. International Journal of Scientific & Technology Research., 674-679.

[13] Almotiri, S. H., Khan, M. A., & Alghamdi, M. A. (2016, August). Mobile Health (m-Health) System in the Context of IoT. IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiClouxdW), (pp. 39-42).

[14] Shafi, G., & Silvio, M. (1984). Probabilistic encryption. Journal of Computer and System Sciences, 270-299.

[15] Gia, T. N., Thanigaivelan, N. K., Rahmani, A. M., Westerlund, T., Liljeberg, P., & Tenhunen, H. (2014). Customizing 6LoWPAN networks towards Internet-of-Things based ubiquitous healthcare systems. Journal of Computer and System Sciences, 1984, 270-299.

[16] Thakre, P. N., & Pokle, S. B. (2022, April). A survey on power allocation in pd-noma for 5g wireless communication systems. In 2022 10th International Conference on Emerging Trends in Engineering and Technology-Signal and Information Processing (ICETET-SIP-22) (pp. 1-5). IEEE.

[17] Thakre, P. N., & Pokle, S. B. (2022). Optimal power allocation for NOMA-based Internet of things over OFDM sub bands. International Journal of Next-Generation Computing, 13(5)..

[18] Yi, X., Paulet, R., & Bertino, E. (2014). Homomorphic Encryption. Homomorphic Encryption and Applications. SpringerBriefs in Computer Science. Springer, Cham., 1118 - 1123.

https://doi.org/10.17993/3cemp.2022.110250.222-230

AUTORS BIOGRAPHY

Ms Palak Vilas Barapatre is pursuing 3rd year B.Tech. in the department of Electronics and communication Engineering, at Shri Ramdeobaba College of Engineering and Management, Nagpur
Email: barapatrepv@rknec.edu

Mr. Yash Jayant Ingolikar is pursuing 3rd year B.Tech. in the department of Electronics and communication Engineering, at Shri Ramdeobaba College of Engineering and Management, Nagpur
Email: ingolikaryj@rknec.edu

Ms Prajakta Milind Desai is pursuing 3rd year B.Tech. in the department of Electronics and communication Engineering, at Shri Ramdeobaba College of Engineering and Management, Nagpur
Email: desaipm@rknec.edu

Ms Pooja Devendra Jajoo is pursuing 3rd year B.Tech. in the department of Electronics and communication Engineering, at Shri Ramdeobaba College of Engineering and Management, Nagpur
Email: jajoopd@rknec.edu

P. N. Thakre has received Bachelor's degree in Electronics Engineering from RTM Nagpur University in 2010. He has done M.Tech. in Electronics Engineering from Shri Guru Gobind Singhji Institute of Engineering and Technology, Nanded University in 2013. Presently he is pursuing Ph. D. from Shri Ramdeobaba College of Engineering and Management, RTM Nagpur University, under the fellowship of Visvesvaraya PhD Scheme for Electronics & IT. His research area includes Non-Orthogonal Multiple Access (NOMA) for 5G Wireless Communication Systems and Wireless channel Estimation Algorithms. Presently he is working as Assistant Professor in Electronics & Communication Engineering Department, Shri Ramdeobaba College of Engineering and Management, Nagpur.

https://doi.org/10.17993/3cemp.2022.110250.222-230