International Journal on Emerging Technologies **11**(2): 140-145(2020)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

A Novel IoT Architecture Based Healthcare Monitoring System

Anil Wamanrao[1] ***and R.L. Raibagkar***[2]
[1]Research Scholar, Department of Post Graduate Studies and Research in Applied Electronics,
Gulbarga University, Kalaburgi-585106 (Karnataka), India.
[2]Professor, Department of Post Graduate Studies and Research in Applied Electronics,
Gulbarga University, Kalaburgi-585106 (Karnataka), India.

(Corresponding author: Anil Wamanrao)
(Received 31 December 2019, Revised 01 February 2020, Accepted 11 February 2020)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: A secured remote patient healthcare ecosystem consisting of heterogeneous devices is implemented by considering three physiological parameters as a blood pressure, pulse rate and body temperature with a camera for patient visualization. A colossal sensor data and camera act as an input to the Raspberry PI where aggregated data is translated for the processing. The processed data is secured for transmission so to avoid different threats and made available for the decision making. To make data secure by a conventional cryptography, the resource constraint of the biomedical devices in IoT environment are not feasible. This is due to the requirement of high power, more space in the memory and higher bandwidth. In the present architecture, a lightweight cryptography algorithm based on advanced encryption system is used, which is implemented using a open source Linux operating system with Libgcrypt cryptography, having its advantage of support of encapsulation for low level cryptography and a low power consumption. It can be modified and redistributed, fully thread safe and easy for interoperability of heterogeneous devices. Confidentiality, data integrity and authenticity among the IoT devices is achieved by the secure communication. Different testing's are conducted with web application tool OWASP ZAP. The use of LAMP domain open source software at all level reduced the total cost of this robust ecosystem.

Keywords: Cryptography, Internet of Things, LAMP domain, OWASP ZAP, Remote Healthcare System and Secure ecosystem.

Abbreviations: IoT, Internet of Things; OWASP ZAP, Open Web Application Security Project Zed Attack Proxy.

I. INTRODUCTION

The IoT has incredible potential to transform human lives by empowering the individual in a near future. It will transform into an internet of service for many of us our things recede into the background and form an integrated service platform. Though it requires data access of each sensor or group of sensor individually an integrated system of systems will make available an architecture enabling us to control our world of service remotely from our tablets, smart phones and other smart devices [1-3]. Advantages of power of IoT in healthcare creates an opportunities for the development of human lifestyle. It opens many doors in healthcare which plays prominent role in wide range of applications. In remote patient healthcare monitoring system, a major issue of secure data transmission to destination and provision to allow only authorized user to access is a challenging task [4-6]. Hence, security is only the concern to address. There are different lightweight cryptographic algorithms like AES, HEIGHT, TEA, PRESENT, RC5 and so forth, are successfully used [7]. Some of the algorithms are hardware or it can be software dependent. Result of the particular method may differ from other by having changes in hardware or software and depending upon the application, adjustment can be done. However, no settled outcome for any algorithm utilizing parameters like clock cycle, memory and latency, etc. the comparative study of the different algorithms shows improvement in aftereffects of a particular lightweight algorithm which leads to IoT innovation for model security with a small size memory space and less utilization of power [8-10]. The Libgcrypt library is used in our system due to more number of advantages [11-13]. Such as: (1) End-to-End communication (2) Low resource network devices (3) Availability of free software (4) Easy for encapsulation (5) supports low level cryptography and (6) Fully thread safe. For the secure communication in IoT, battery powered devices are used and since it requires communication with many devices with less power available which is possible due to lightweight cryptography. IoT gives birth to new requirements like security and power requirement. It is feasible to design lightweight cryptography that needs fewer resources with no compromise in security level. The study reported shows there is use of privilege software or use of more hardware devices which leads to increase in cost [14-16]. In this study the total use of open source software at all levels and minimum use of hardware for the same results, which implies reduced cost of the system.

II. DESIGN AND DEVELOPMENT OF REMOTE BASED HEALTHCARE SYSTEM

The remote healthcare monitoring system operating with the signal path is shown in Fig. 1 [17].

Fig. 2 depicts the data collection phase where data is acquired by sensor with camera which is shown in Fig. 2. In embedded system different domain devices come together to exchange data which needs further processing.

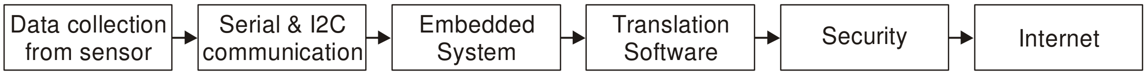


Fig. 1. Signal path in remote healthcare system.

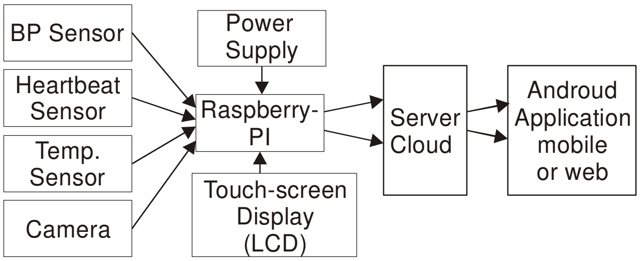


Fig. 2. Basic block diagram for remote healthcare system.

III. SECURITY

Raspberry-pi supports both wired and wireless communication also it provides audio, video output ports by HDMI and Ethernet for the internet connections [18-19]. Raspberry pi where data's are collected and processed for remote application by software gateways is to upload and retrieve the data with a lightweight cryptography using Libgcrypt library as shown in Fig. 3 and 4.

(a) Base Station

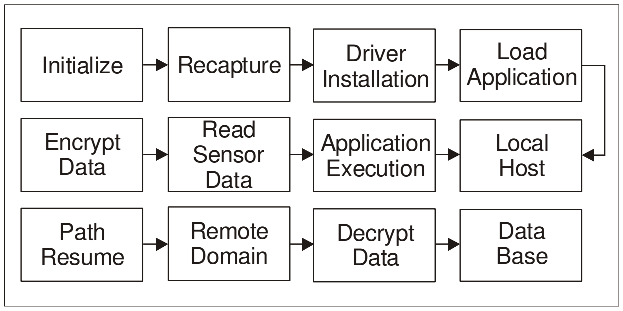


Fig. 3. Base station flow diagram for remote healthcare system.

(b) Remote Station

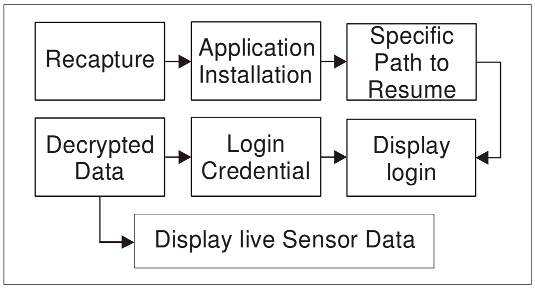


Fig. 4. Remote station flow diagram for remote healthcare system.

The processing of data is carried out by embedded processor, which will be transmitted to remote devices to communicate by internet [20-23]. The signal passes by internet path is vulnerable to the number of threats, to overcome this issue, security becomes more important. Without security mechanism the IoT will not be pervasive as it is anticipated. Mainly there are two requirements one is real time and other is security with confidentiality.

Linux OS on Raspberry pi: For high level applications in embedded system it is reported that the Raspberry pi is used with Windows10 IoT core for small ARM and x86/x64 devices. The work is to evaluate the extent to which Raspberry PI is portable system as ready to compare with desktop computers [24]. In other healthcare application TinyOS is implemented. This is designed mainly for embedded sensor network [25]. This architecture is component based, which will minimize the code size. In this it is difficult to reconfigure online addition of devices.

In our project remote healthcare monitoring needs real-time systems which has less latency time and meet the deadline as predefined. The OS used is Linux due to its properties like quality and reliability and is an open source development model. Availability of code has implications of commoditization of components. This operating system broadly supports for different hardware platforms and portability.

The study shows that higher end development board like Raspberry-pi have higher performance in comparison with arduino in terms of computing speed and storage. In addition, the Raspberry-pi equipped with the in-built Bluetooth and wifi serves as easy to connect to the internet and upload the data to the cloud server if required for further processing.

Apache for the web server application is implemented which is also supports for MySQL. PHP is used for the server side for dynamic database interaction, which is for web based software application [26].

IV. LIGHTWEIGHT CRYPTOGRAPHY

The cryptographic algorithm is needed for the secured communication. Secured communication provides no modification of data by unauthorized use.

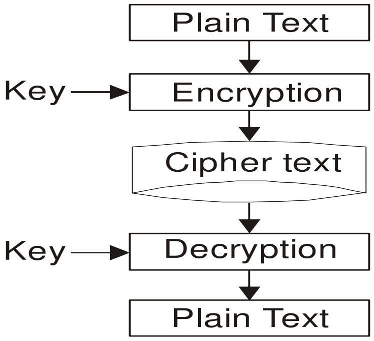


Fig. 5. Cryptographic algorithm.

The cryptography is a technique of mixing logical and mathematical function for encryption and decryption and is shown in Fig. 5. Access of the patient data is a personal right. Therefore the system requires secure data transfer where three aspects are considered to be important are confidentiality, privacy and security. In addition for the quality service requires authentication, authorization, integrity, interoperability, reliability, resource efficiency and access control [27, 28].

Any application deal with remote healthcare system requires to achieving physical and technological security measure constraints such as:

– Electronic objects: There should be authorize data access health centers. Any electronic hardware removing, transferring and re-using must ensure previously established security.

– Software implemented: Needs only authorized person can access data at the authorized healthcare centre by providing unique user ID and atomic password.

– However it must have provision for encrypted data storage and log-off automatic

– Routine activity database: Design should be capable to preserve login and logout data, which will be helpful to recognize security breach latter.

– System recovery: System must have back-up storage of patient data. In case system software failure it must be capable to recover patient data.

– Network security: Eavesdropping, data tampering and un-authorized access are the important measures to protect

In IoT environment there is need of end point secured communication. If anyone node fails to provide security the whole network will suffer to meet security requirement.

However, there are limitations to implement cryptographic algorithm on the object connected due to their resources. The resources constrained are less bandwidth, less power and less memory capacity available. Hence, an efficient security is required which will not suffer due to resources of IoT. There are solutions to these wireless networks which require resource efficient. Whenever large networks are to be implemented, security becomes a prominent issue to deal. In a remote healthcare system human health related data are to be collected for transmission which is vulnerable to a highest privacy concerns. Since the network involved in communication is a wireless network. Being a human health related data a robust communication among sensor, actuator and distant doctor is a sensitive issue. Any type theft of data, keeps the people away from remote healthcare system. As the sensor lacks memory, power, bandwidth, they can easily be lost because of the small size [29-30]. To overcome many of above constrains we have implemented libgcrypt cryptography.

Libgcrypt is a general purpose cryptography which functions for many cryptography methods and modes which also supports hash algorithms, MAC's, public key algorithm, large integer functions and random numbers [31]. It will work on POSIX and pre-POSIX system and even it will be designed for cross compiler. It has got its own multiple precision arithmetic implementation having capable with assembler support to many processors. It is developed in C language in open source mode. The source code size is 216 and code line to comment line ratio is 6.27. Libgcrypt is portable, thereby it will be implemented on 32 and 64 bit processor, unix system, win32, win64 and wince and so on. It has hardware-assisted support by which it can use specific hardware assistance to achieve greater speed and improved security. For SIM, smartcard and HSM protocol it will be supported.

Threat Analysis: IoT ecosystem needs interaction of more devices and hence data acquired is required to protect. Depending upon the application, significance of threat varies from application to application [24]. In the data storage, stored information in memory may be attacked or changed. The modified or changed data is used for analysis will give different results. However, the libgcrypt has got provision to protect storage memory devices from the attack. It needs pre-defined memory size because any operating system will have a need of definite size of memory storage. This initialization can be done by application, since this option is not available in other library. Therefore Libgcrypt provides secured memory storage for information and key.

Research methodology: Analysis starts with known security threats in the IoT medium and examines to provide security mechanism in IoT to guard against these threats. By employing suitable operating platform and cryptographic algorithm is implemented to achieve secure data communication with privacy, confidentiality, data integrity and authenticity among the IoT devices. Also, emphasis on the execution speed with the available sources and optimization of different parameters such as time, throughput, speed and efficiency are taken care.

V. ANLYSIS OF THE SYSTEM PERFORMANCE

The complete hardware of the system designed with a pictorial view is shown in Fig. 6 and Table 1 shows the blood pressure standards of the American Heart Association chart. This is considered as a standard for the systolic and diastolic blood pressure. Doctor can observe the readings from android application mobile as shown in Fig. 7 and 8 of the two patients.

(a) Experimental set-up

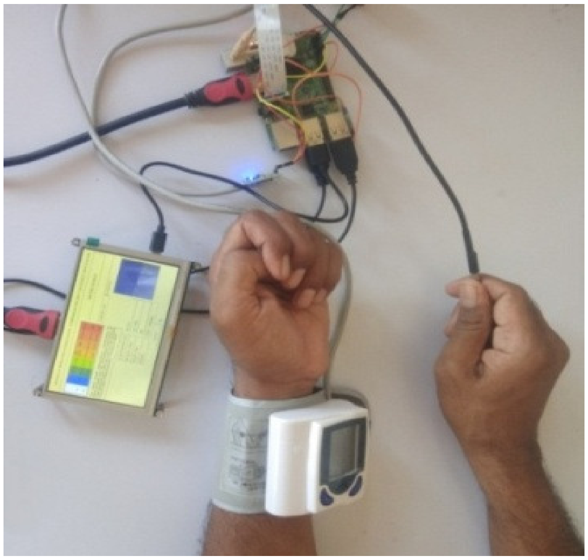
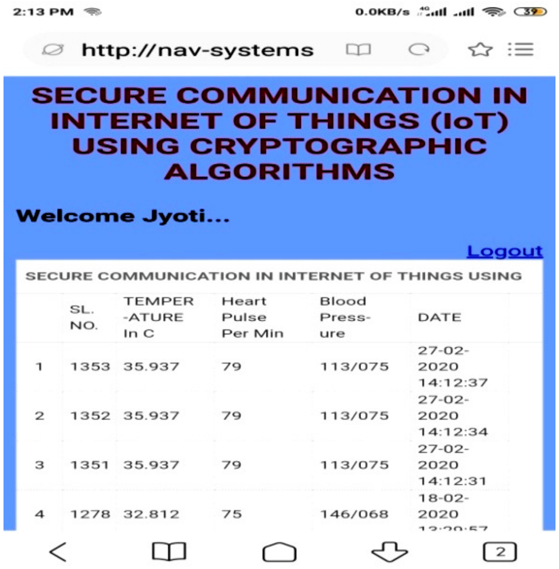


Fig. 6. Remote Healthcare Monitoring.

Table 1: Blood pressure standards of AHS.

Blood Pressure Category	Systolic mm Hg (upper number)	Diastolic mm Hg (lower number)
Normal	Less than 120	Less than 80
Elevated	120-129	Less than 80
High Blood Pressure (Hypertension) Stage 1	130-139	80-89
High Blood Pressure (Hypertension) Stage 1	140 or Higher	90 or higher



SECURE COMMUNICATION IN INTERNET OF THINGS (IoT) USING CRYPTOGRAPHIC ALGORITHMS

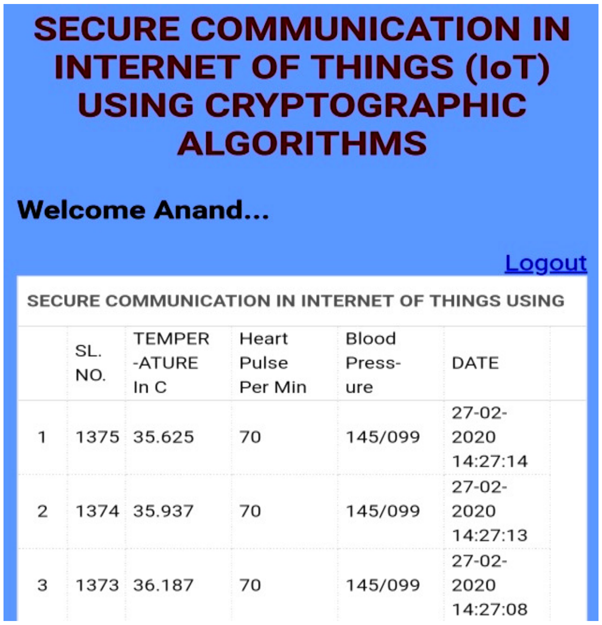
Welcome Jyoti...

Logout

SECURE COMMUNICATION IN INTERNET OF THINGS USING

	SL. NO.	TEMPER -ATURE In C	Heart Pulse Per Min	Blood Press-ure	DATE
1	1353	35.937	79	113/075	27-02-2020 14:12:37
2	1352	35.937	79	113/075	27-02-2020 14:12:34
3	1351	35.937	79	113/075	27-02-2020 14:12:31
4	1278	32.812	75	146/068	18-02-2020 12:20:57

Fig. 7. Remote Android Mobile Data patient 1.



SECURE COMMUNICATION IN INTERNET OF THINGS (IoT) USING CRYPTOGRAPHIC ALGORITHMS

Welcome Anand...

Logout

SECURE COMMUNICATION IN INTERNET OF THINGS USING

	SL. NO.	TEMPER -ATURE In C	Heart Pulse Per Min	Blood Press-ure	DATE
1	1375	35.625	70	145/099	27-02-2020 14:27:14
2	1374	35.937	70	145/099	27-02-2020 14:27:13
3	1373	36.187	70	145/099	27-02-2020 14:27:08

Fig. 9. Remote Android Mobile Data patient 2.

VI. TESTING

Vulnerabilities in web application: The main objective of the OWASP ZAP testing is to find vulnerabilities in web site. Therefore we have developed our site of which vulnerabilities were tested using ZAP. It is successfully found different kind of vulnerabilities in the web site as shown in Table 2. It will not find only vulnerabilities but also suggest how to overcome

Table 2: Summary of alerts.

S. No.	Risk level	No. of alerts
1	High priority	0
2	Medium Priority	1
3	Low priority	3
4	Informational	0

System test cases: This test is to verify compliance against a specific requirement of pre and post conditions and expected results. The system designed is tested to check whether system meets the functional requirements. The test results are shown in Table 3, 4 and 5.

Table 3: Case 1: Map-reading from login to monitor page.

Condition	Input side	Output side	Expected result (Y/N)
User on login page	Click on login page	Appeared on monitor page	Y

Table 4: Case 2: Map-reading from monitoring to Google page.

Condition	Input side	Output side	Expected result (Y/N)
User on monitor page	Click on location link	Appeared on Google page	Y

Table 5: Case 3: Map-reading from Google to monitor page.

Condition	Input side	Output side	Expected result (Y/N)
User on Google page	Click on monitor page link	Appeared on monitor page	Y

VII. CONCLUSION

The main requirements are security and privacy since from the beginning of digital data transmission. But the research in technology results so many changes in different fields in particular IoT finds many applications to improve lifestyle of human being. IoT innovation gives birth to remote healthcare monitoring system due to its architecture and solutions for different methods.

Open source platforms and operating system can improve security, quality and availability of remote healthcare system. It will also improve the evolution and efficiency by enabling security for the devices. This implies that there is a enhancement in interoperability and decrease in cost management.

This paper presents a secure remote healthcare monitoring system implementation using sensors colossal data as input to the Raspberry-pi. This aggregated data is translated for the processing. In this architecture a lightweight cryptography algorithm based on the advanced encryption system is implemented with the use of Libgcrypt.

The Raspberry-pi MAC address facilitates to connect website through internet and upload the patients data. The doctor at remote distance can observe patients physiological parameters on the website or mobile application which is implemented using LAMP domain. For the testing website OWASP ZAP is used which is an open source software/tool. Since the use of open source software at different levels with an embedded hardware system in the IoT environment reduces the total cost of the project.

VIII. FUTURE SCOPE

By the addition of more number of sensors to consider other physiological parameters such as ECG, EEG and oxygen saturation and more can be implemented for the detail study about the patient. Also to make the system more robust another testing can be performed using Burp suite software/tool.

Conflict of Interest. The authors declare no conflict of interest.

REFERENCES

[1]. Alzubi, J. A., Manikandan, R., Alzubi, O. A., Gayathri, N., & Patan, R. (2019). A Survey of Specific IoT Applications. *International Journal on Emerging Technologies, 10*(1), 47-53.

[2]. Gómez, J. E., Oviedo, B., & Zhuma, E. (2016). Patient Monitoring System Based on Internet of Things. *Procedia Computer Science, 83*, 90-97.

[3]. McEwen, A., & Cassimally, H. (2013). *Designing the internet of things*. John Wiley & Sons.

[4]. Kamal, R. (2017). Internet of Things Architecture and Design Principles, McGraw Hill Education (India) Private Limited.

[5]. Tripathy, B. K., & Anuradha, J. (Eds.). (2018). *Internet of Things (IoT): Technologies, Applications, Challenges and Solutions*. CRC Press.

[6]. Patil, A. W., & Raibagkar, R. L. (2019). An IoT based Real Time Health Monitoring System with Secure Communication Using Cryptographic Algorithms. In *International Journal of Electronics Engineering, 11*(1), 96-99.

[7]. Buchanan, W. J., Li, S., & Asif, R. (2017). Lightweight cryptography methods. *Journal of Cyber Security Technology*, *1*(3-4), 187-201.

[8]. Hameed, S., Khan, F. I., & Hameed, B. (2019). Understanding security requirements and challenges in Internet of Things (IoT): A review. *Journal of Computer Networks and Communications*, 1-14.

[9]. Santhoshkumar, S., Mohamed, A. T., & Ramaraj, E. (2019). Process Analytics Model for Health Care using IoT and Big Data Techniques. *International Journal on Emerging Technologies, 10*(4), 197-200.

[10]. Almotiri, S. H., Khan, M. A., & Alghamdi, M. A. (2016). Mobile health (m-health) system in the context of IoT. In *2016 IEEE 4th International conference on future internet of things and cloud workshops (FiCloudW)* (pp. 39-42). IEEE.

[11]. Abood, O. G., & Guirguis, S. K. (2018). A survey on cryptography algorithms. *International Journal of Scientific and Research Publications*, *8*(7), 495-516.

[12]. GNU Privacy Guard URL https://www.gnupg.org

[13]. GNUPGFrontends,URLhttps://www.gnupg.org/related_software/frontends.html.

[14]. Ganesh, E. N. (2019). Health Monitoring System using Raspberry pi and IoT. *Oriental Journal of Computer Science and Technology, 12*(1), 8-13.

[15]. Mohammad Dawood Babakerkhell & Pandey, N. (2019). Analysis of Different IoT Based Healthcare Monitoring Systems. *International Journal of Innovative Technology and Exploring Engineering*, *8*, 61-67.

[16]. Muqeet, M. A., & Quadri, M. U. (2019). IoT based Patient Monitoring System Using Raspberry Pi. *International Journal of Research in Electronics and Computer Engineering*, *7*, 2976-2980.

[17]. Baig, M. M., Gholam Hosseini, H., Moqeem, A. A., Mirza, F., & Lindén, M. (2017). A systematic review of wearable patient monitoring systems–current challenges and opportunities for clinical adoption. *Journal of Medical Systems*, *41*(7), 1-9.

[18]. Rajpoot, S. S., & Khandelwal, A. (2018). Home Energy Control System Using Wireless Smart Socket and IoT. *International Journal of Electrical, Electronics and Computer Engineering*, *7*(1), 14-20.

[19]. Flauzac, O., Gonzalez, C., & Nolot, F. (2016). Developing a distributed software defined networking testbed for IoT. *Procedia Computer Science*, *83*, 680-684.

[20]. Zanjal, S. V., & Talmale, G. R. (2016). Medicine reminder and monitoring system for secure health using IOT. *Procedia Computer Science*, *78*(3), 471-476.

[21]. Tao Du, Shouning Qu, Kaiqiang Liu, Jinwen Xu, Yinghua Cao (2016). An efficient data aggregation algorithm for WSNs based on dynamic message list, *Procedia Computer Science*, *83*, 98-106.

[22]. Bayo-Monton, J. L., Martinez-Millana, A., Han, W., Fernandez-Llatas, C., Sun, Y., & Traver, V. (2018). Wearable sensors integrated with Internet of Things for advancing eHealth care. *Sensors*, *18*(6), 1-14.

[23]. Pathak, P., & Quaz, M. A. (2017). Issues, Challenges and Solution for Security in Wireless Sensor Networks: A Review. *International Journal of Electrical, Electronics and Computer Engineering*, *6*(1), 4-11

[24]. Hao, Y., & Foster, R. (2008). Wireless body sensor networks for health-monitoring applications. *Physiological measurement*, *29*(11), 1-42.

[25]. Koshti, M., Ganorkar, S., & Chiari, L. (2016). IoT Based Health Monitoring System by Using Raspberry Pi and ECG Signal. *International Journal of Innovative Research in Science, Engineering and Technology*, *5*(5), 8977-8985.

[26]. Keoh, S. L., Kumar, S. S., & Tschofenig, H. (2014). Securing the internet of things: A standardization perspective. *IEEE Internet of things Journal*, *1*(3), 265-275.

[27]. Darshan, K. R., & Anandakumar, K. R. (2015). A comprehensive review on usage of Internet of Things (IoT) in healthcare system. In *2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)* (pp. 132-136). IEEE.

[28]. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-

Things. *IEEE Internet of Things Journal*, *4*(5), 1250-1258.

[29]. Rahimi Moosavi, S., Nguyen Gia, T., Rahmani, A. M., Nigussie, E., Virtanen, S., Isoaho, J., & Tenhunen, H. (2015). SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. In *Procedia Computer Science*, *52*, 452-459. Elsevier.

[30]. Usman, M., Ahmed, I., Aslam, M. I., Khan, S., & Shah, U. A. (2017). SIT: a lightweight encryption algorithm for secure internet of things. In *International Journal of Advanced Computer Science and Applications*, *8*(1), 1-10.

[31]. Shah, A., & Engineer, M. (2019). A survey of lightweight cryptographic algorithms for IOT-based applications. In *Smart Innovations in Communication and Computational Sciences*, 283-293. Springer, Singapore.

How to cite this article: Wamanrao, Anil and Raibagkar, R. L. (2020). A Novel IoT Architecture Based Healthcare Monitoring System. *International Journal on Emerging Technologies*, *11*(2): 140–145.