International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 11 • Issue 1 pp. 96-99 Jan 2019-June 2019 www.csjournals.com

An IoT based Real Time Health Monitoring System with Secure Communication Using Cryptographic Algorithms

Anil Wamanrao Patil[1], and R. L. Raibagkar[2]
[12]Departmentof Post Graduate Studies and Research in Applied Electronics,
Kalaburagi - 585106, India.
email- awpatil01@gmail.com and raibagkarrl@gmail.com

Abstract: To reduce the human error of collecting data, IoT makes medical equipment more efficient by allowing real time monitoring of patient health. IoT based patient health tracking system effectively uses internet to monitor patient health status and save lives on time. Here we report the development of an IoT based cryptographic algorithm. At the patients location (Master device), all the sensors information is encrypted with s-key and results as cipher text. The secured information cannot be encoded by any other user unless the encryption algorithm and key streams are leaked out. The secured text will be decoded by the IoT client application system and returns the plain text at the device only. Thus, the data can be transferred between the master device and client application device in secure manner.

Keywords: Cryptographic algorithm, Health Monitoring system, IoT and Sensors.

Introduction

IoT is subject of rising interest for its fundamental significance and its technological development in creating new algorithms, software, hardware and its applications both in science and engineering [1-3]. The purpose this paper is to report the development of such IoT based real time monitoring system with secure communication employing cryptographic algorithms for continuous monitoring of some of the physical parameters such as human body temperature, blood temperature and pulse rate.

A LCD display at the patient is made available for the display of patient health parameter for the medical practitioner or nurse attendant. Different sensors provide analog data signal which is converted into digital signal which is given as input to the Raspberry- PI. Similarly, in a tiny platform it provides a very low cost platform for Linux server. The general purpose input output pins of the Raspberry- PI allows interfacing of sensors. The data available through Raspberry- PI is given to registered MAC address and is further processed.

Methodology

The IoT concept begin with object classified as identity communication devices. Objects or things are connected for these devices for their identification which can be tracked, controlled and monitered using distant computers connected through internet. Figure 1 shows IoT based health care system developed to control geological parameters of the patient such as temperature,blood pressure and pulse rate indicator.

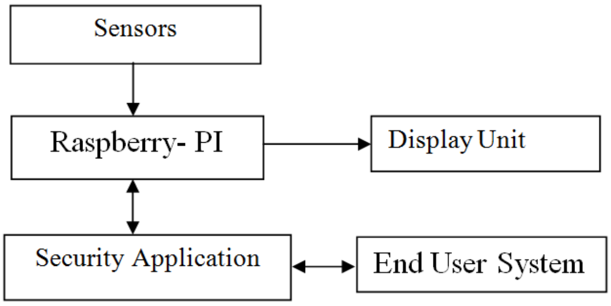

Figure 1. Block diagram of patient health center system

In addition to data security, a LCD display is also provided at the patient side to display the physiological parameter of the patient. By looking into the real time data and physical condition of patient by camera a doctor at remote can communicate to the attendant doctor or nurse. Camera and LCD display at the patient side and android application mobile at the doctor side is provided for conversation between patient attendant doctor and specialist doctor real time and secure.

Security

Security requirements at different level need different issues and several were reported [4, 5] Cryptographic algorithm and key management is the main feature of our system.

Cryptographic algorithm

Light weight cryptographic is an advance technique on attack, design and implementation [6-9]. This technique can be implemented in constrained environment of contactless communication [10, 11].Basically this technique delivers adequate security. Recently used technologies of light weight cryptographic primitives are symmetric key cryptographic and public key cryptography [12]. However symmetric cryptography, have three types as block ciphers, stream ciphers and hash functions light weight [13]. With this, it is possible to have end-to-end communication efficiently with low power consumption. Another reason is due to its capability of more number of network connection by having less number of resource devices.

In our system, we have implemented the encoding and decoding of data as per the flow charts shown in Figure 2 and Figure 3. To start with we need to initialize the Raspberry- PI board with power supply, Sensor controller board, temperature Sensor, heart beat sensor, BP Sensor, Pulse Sensor, Wi-Fi, Laptop and LCD display. Then we boot the Raspberry –PI with operating system installed on SD Card. So that, all the driver software starts driving sensors connected to achieve communication with Raspberry-PI and Sensors. After the software initialization, application codes were loaded into SD card. The same can be achieved by laptop where we develop application program and transfer it to SD card using USB file transfer adapter. To set a local server, PHP Source code on-to the domain control panel and Qt libraries on Linux operating system were initialized.

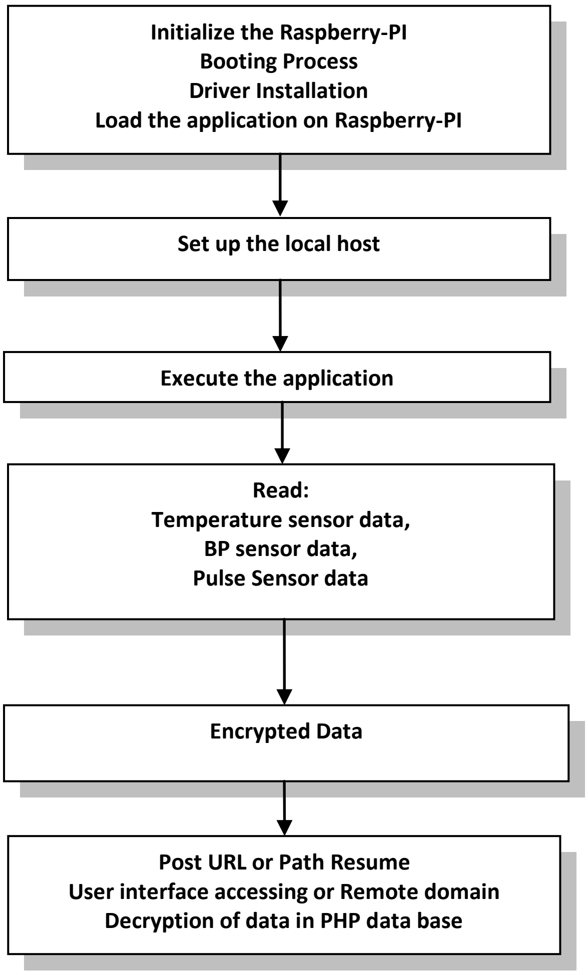

Figure 2. Flowchart for uploading the data

Once the server is setup the application software is executed to collect the data from temperature sensor, heart beat sensor, BP Sensor and Pulse Sensor, which is further encrypted. The encryption is carried out by encryption algorithm and secrete key (s-key). All encrypted data string is posted to the domain URL with REST API method or HTTP[14, 15]. For transmitting data, Wget-post is used to remote domain server. The same data is retrieved in local host server by decryption with authorized key and saved it to database. S-key is based on the GnuPG which is a code derived from general purpose cryptographic library Libgcrypt.

Libgcrypt has the functionalities like all cryptographic building blocks and symmetric cipher algorithms. All the four sensor data acquired by Raspberry- PI as per the available GPIO and UART pins connectivity are connected to standard identifier string which is plain text to transmit to website. Connections are established appended the key stream or encryption password to the plain text and applied through Libgcrypt library. Hence the encrypted string from the s-key is generated. The REST method for HTTP protocol sends encrypted string to PHP script.

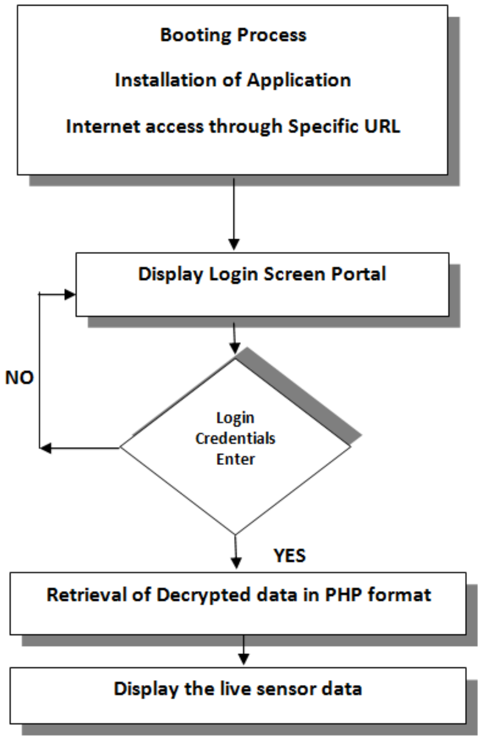
Booting Process
Installation of Application
Internet access through Specific URL
Display Login Screen Portal
NO
Login Credentials Enter
YES
Retrieval of Decrypted data in PHP format
Display the live sensor data

Figure 3. Flowchart of data processing at client side

At the client side, the application programme is loaded into web server root directory of the web hosting server. The domain specific URL access to display login screen portal, to read sensor data from the system connected to web server script. Hence, live sensor data is available on the web page captured from the patient for all parameters. With password, plain text is extracted from encrypted string by decryption and finally the plain text is saved into the database for further analysis.

Conclusion

We have successfully used light weight cryptography using s-key management technique, which is more precise and secure than centralized delegation based architecture. Due to this technique it has more resilience over denial of service attack. The s-key management technique is a very promising solution to provide reliable security for IoT based health care System**.**

Acknowledgement

The author acknowledges the management of Basavakalyan Educational Trust, Basavakalyan for providing constant support for research work.

References

[1]. A M Rahmani, N K Thanigaivelan, T N Gia, Jose Granados, B Negash, Pasi Liljeberg and Hannu Tenhunen, “Smart e-health gateway: Bringing intelligence to internet-of- things based ubiquitous healthcare systems”, 12th Annual IEEE, Consumer Communications and Networking Conference (CCNC), pp.826-834, 2015.

[2]. A Kulkarni and S Sathe, “Healthcare applications of the Internet of Things: A Review”, International Journal of Computer Science and Information Technologies, vol. 5, No. 5, pp.6229-6232, 2014.

[3]. C Li, X Hu and L Zhang, “The IoT-based heart disease monitoring system for pervasive healthcare service”, Procedia Computer Science, vol.1, no.12, pp.2328-2334, 2017.

[4]. S R Moosavi, T N Gia, A M Rahmani, E Nigussie, S Virtanen, J Isoaho and H Tenhunen, “SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways”, Procedia Computer Science, Vol. 52, pp.452-459, 2015.

[5]. H Suo, J Wan, C Zou and J Liu, "Security in the internet of things: a review, "International conference on Computer Science and Electronics Engineering (ICCSEE), Vol. 3, pp. 648-651, IEEE, 2012.

[6]. S L Keoh, S S Kumar and H Tschofenig. "Securing the internet of things: A standardization perspective", IEEE Internet of Things Journal, vol. 1, no. 3, pp. 1-12, 2014.

[7]. M Katagi and S Moriai, "Lightweight Cryptography for the internet of things", Sony Corporation, pp.7-10, 2008.

[8]. Isha and A K Luhach, "Analysis of lightweight cryptographic solutions for Internet of Things, "Indian Journal of Science and Technology, vol. 9, no.28, pp. 1-7, 2016.

[9]. S H Almotiri, M A Khan and M A Alghamdi, "Mobile health (m-health) system in the context of IoT" International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pp. 39-42, IEEE, 2016.

[10]. A Sawand, S Djahel, Z Zhang and F N Abdesselam, "Toward energy-efficient and trustworthy e Health monitoring system", China Communications, vol. 12, 2015.

[11]. J. Sathish Kumar and D R Patel, "A survey on internet of things: Security and privacy issues", International Journal of Computer Applications, vol. 90, no.11, pp.20-26, 2014.

[12]. A Rghioui, A L'aarje, F Elouaai and M Bouhorma, "The internet of things for healthcare monitoring: Security review and proposed solution", Third IEEE International Colloquium in Information Science and Technology (CIST), IEEE, pp. 384-389, 2014.

[13]. M Usman, I Ahmed, M I Aslam, S Khan and U A Shah, "SIT: A lightweight encryption algorithm for secure internet of things", vol. 8, no.1, pp.1-10, 2017.

[14]. D Lake, R Milito, M Morrow and R Vargheese, "Internet of things: Architectural frame work for e-health security", Journal of ICT, vol. 3 & 4, pp. 301-328, 2014.

[15]. S A Kumar, T Vealey and H Srivastava, "Security in internet of things: Challenges, solutions and future directions", 49th Hawaii International Conference on System Sciences (HICSS), IEEE, pp. 5772-5781, 2016.