International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 3, ISSN No. 2455-2143, Pages 79-82
Published Online July 2022 in IJEAST (http://www.ijeast.com)

DATA SECURITY IN HEALTHCARE USING IOT

Krithick J G, Nivedh T S, Siva Bharath S
(B.E Students, Department of ECE)
Amrita College of engineering & technology, nagercoil

Dr. Radhamani.A. S,
M.E, Ph. D, Assistant Professor, Department of ECE,
Amrita College of engineering & technology, nagercoil

Mr.V.Ramanathan,
M.E, Assistant Professor, Department of ECE,
Amrita College of engineering & technology, nagercoil

***Abstract:* While the Internet of Things (IoT) has been instrumental in healthcare data transmission, it also presents vulnerabilities and security risks to patients' personalized health information for remote medical treatment. Currently most published security solutions available for healthcare data don't seem to be focused on data flow all the way from IoT sensor devices placed on a patient's body through network routers to doctor's offices. In this project, the IoT network facilitates healthcare data transmission for remote medical treatment, explored security risks related to unsecured data transmission, especially between IoT sensor devices and network routers, then proposed an encrypted security solution initiated at IoT sensor devices. Our proposed solution provides a cryptography algorithm embedded into the sensor device such that packets generated with patient's health data are encrypted right at the sensor device before being transmitted. The proof of concept has been verified employing a lab setup with two level encryption at the IoT sensor level and two level decryption at the receiving end at the doctor's office. Test results are promising for an end to-end security solution of healthcare data transmission in IoT. This project also provides further research avenues on IoT sensor driven security.**

***Keywords*: IoT, Sensor, Data Security and Network Routers.**

I. INTRODUCTION

Health is characterized as a full state of physical, mental, and social well-being and not merely a lack of illness. Health is a fundamental element of people's need for a better life. Unfortunately, the global health problem has created a dilemma because of certain factors, such as poor health services, the presence of large gaps between rural and urban areas, physicians, and nurses unavailability during the hardest time.

With the rapid advancement of technology, the Internet of Things (IoT) has become a common and efficient method to store information securely in recent times. IoT is the practice of connecting devices via the Internet, ranging from cell phones, electronic devices, wearable devices, etc. An IoT network system consists of the following components: sensor devices, connectivity, data processing, and user interface. First, healthcare data e.g. heart rate, blood sugar, etc. is collected through sensor devices. It is then transmitted by using radio access points to the cloud network and then processed as designed for specific application. Lastly, the user interface plays its part to make the information useful to the end user.

The increasing benefits of data transmission using IoT has prompted the healthcare sector to adapt to cloud networking and utilize it to make the process of healthcare more accessible and efficient. To design a smart healthcare system in IoT environment that can monitor a patient's basic health signs in secure manner. In this system, two sensors are used to capture the data from hospital environment named heart beat sensor and body temperature sensor. The condition of the patients is conveyed via a portal to medical staff, where they can process and analyze the current situation of the patients.

II. EXISTING SYSTEM

The present patient monitor systems in hospitals allow continuous monitoring of patient vital signs, which require the sensors to be hardwired to nearby, bedside monitors or PCs, and essentially confine the patient to his hospital bed. Even after connecting these systems to a particular patient, a paramedical assistant is needed to continuously monitor and note down all the vital parameters of a given patient by keeping track of all of his/her records manually. Adopting such a method is error prone and may lead to disaster in the case of a human error. In the existing system the patient health is continuously monitored by the Mobile multi patient monitoring system and the acquired data is transmitted to a centralized ARM server using Wireless Sensor Networks. A ZigBee node is connected to every patient monitor system that consumes very low power and is extremely small in size. These are specifically designed for low power consumption, with minimal circuit components intended for small packet, long distance range applications and typically consist of a low power processor with minimal resources and interface capabilities. They also have a conservative transceiver that is capable of transmitting 8 bytes of data at a time and has a moderate transmitting range of about 130 m. Therefore, WPANs seem to be a perfect fit for remote patient monitoring.

III. PROPOSED SYSTEM

Proposed system provides a cryptographic algorithm embedded into the sensor device such that the packets generated with patient's health data are encrypted right at the sensor device before being transmitted. To explain the cryptographic mechanism used in mathematical terms, we multiply the sensor-collected data in the form of an m by n matrix with a cryptographic key-code matrix to encode the message in encrypted data. This encrypted information transmits securely from IoT sensor to the access point, from the access point to cloud, and then from cloud all the way to doctor's office. At the doctor's end terminal, the data gets decrypted by multiplying with the inverse of the original cryptographic key-code to decode patient data. The unique advantage of our solution, as emphasized previously, is ensuring an encrypted data flow all the way from IoT sensor devices placed on the patient's body through network routers to doctor's offices. Another notable advantage is the method of data encryption being used. Most existing solutions, as shown in Figure 2 below, encrypt the data by adding the message and the key that while being sent on air makes it easy for hackers to manipulate and access the secured data without investing a lot of time or knowledge. Our proposed solution, on the other hand, encodes the information by multiplying the message and key in such a manner that it is not easily identifiable by an outsider to the system. As shown below, the output message is completely different from the original input and key, making the protocol very secure and safe from intruders. While our solution takes care of security-related issues directly from IoT sensor device level to doctor's access routers, priority routing of healthcare data packet is another key area under investigation. It has been published as part of our separate research and focuses on sensor driven solution to prioritize healthcare data routing in congested IoT networks by adding an identifier at the sensor level and prioritizing the data based on the identifier.

IV. SYSTEM ARCHITECTURE

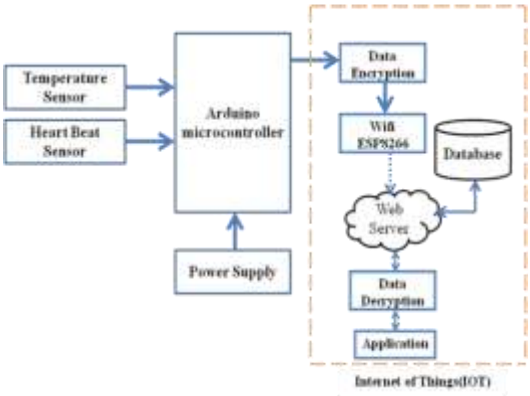


Fig.1. System Architecture

V. RESULT AND DISCUSSION

The developed system was tested with various subjects of different ages in different conditions. In the test cases, for heartbeat and body temperature we manually calculated the actual value and observed value from the developed system. The sensors are wired which are used to collect data from the patient's body and the environment by gathering physiological signs. The collected data are then processed via an ESP32 module and send to the gateway server. For the web user interface, ASP is used for the graphical interpretation, and display of collected results. ASP shows the current status and process of transactions. The HTTP protocol provides easy connectivity for the correspondence between a Wi-Fi module and the web server. The HTML user interface is updated every 15 s, allowing patients to be tracked in real-time. The main advantage of our proposed end-to-end IoT security control scheme is that its implementation is at the source and destination node level, making it easy for implementation and has the advantage of avoiding extra delay at the middle hop nodes

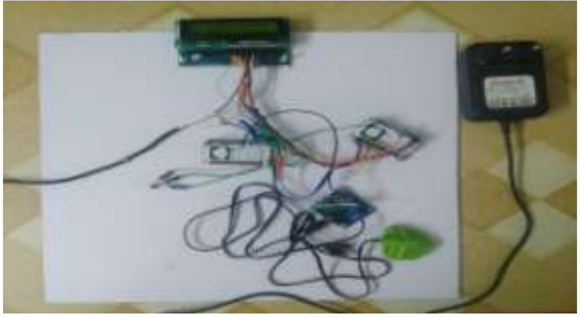
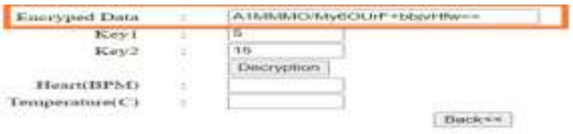


Fig.2. Prototype

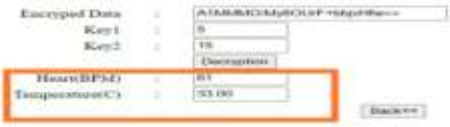
After concluding the set-up of the system, the process is initiated to ensure that the encryption-decryption algorithm works as per stated. It has been tested with different examples to show how it successfully encrypts and decrypts the data on the sender and receiver end, respectively.



Encryped Data : A1MMMO/My6OUrF+bbjvHfw==
Key1 : 5
Key2 : 15
Decryption
Heart(BPM) :
Temperature(C) :
Back<<

Fig.3. Encrypted Data

Generally, we evaluated our algorithm in terms of memory usage, processing time, key size, vulnerability to known attacks, communication overhead, energy consumption, flexibility of application to different IoT types, and cost. Compared to existing security methods, our algorithm has less consumption in energy, processing time and memory. Here, we have tested the system with two different sets of inputs to show how it is encrypted and transmitted over air.



Encryped Data : A1MMMO/My6OUrF+bbjvHfw==
Key1 : 5
Key2 : 15
Decryption
Heart(BPM) : 61
Temperature(C) : 33.00
Back<<

Fig. 4. Decrypted Data

As shown, this method effectively takes the unsecured data and changes it to an unrecognizable format to be transmitted via the IoT network to the receiver and then finally deciphers it on the other end by those who are aware of the system's keys. One major advantage of this algorithm is that it does not make use of built-in keys. Had we made use of built in keys, the system would be understandable by anyone who knows the protocol and would make it easier for hackers to decrypt. By using self-created keys unique to each patient, we are securing our system further from those preying on the data. Additionally, another advantage is that our algorithm implements character by character encryption, making it difficult for a man in the middle to decrypt it. Overall, the algorithm does a good job of identifying the weak security points from the very start and implementing techniques that are simple and yet very difficult to break by hackers who are not aware of its functionalities. Last but not the least, priority is also heavily related to security and that has been researched as part of our separate research that can be combined to provide a much more secure and efficient system.

VI. CONCLUSION

Security is a vital component in healthcare data transmission in the IoT network due to the sensitivity and confidentiality of patient's information. However, certain parts of the data transmission network such as IoT sensor devices on patients' bodies to routers are still unsecured, leaving room for intruders to interfere and misuse the sensitive information. We proposed a security solution with an encryption mechanism embedded into the IoT sensor device such that a patient's health data packet will be encrypted right at the packet transmission initiation point. Our solution attempts to tackle the security issues from the very base so as to not leave any room for third parties preying on the data. By securing data from the sensor device to the cloud using encryption. IoT network, it eliminates any chances of the data being deciphered before reaching the cloud. Similarly, assuming the cloud is already secured with an existing security solution, the data is secured all the way until it reaches its destination such as the doctor's office or medical database and can only be decrypted if the receiver end is aware of the key that was used to encrypt it initially. Our test results are promising for an end-to-end security solution of healthcare data transmission in IoT. This paper also contributes by opening up further research avenues on IoT sensor driven security.

VII. FUTURE WORK

Future work proposes a smart healthcare system in IoT environment that can monitor a patient's basic health signs as well as the room condition where the patients are now in real-time. In this system, five sensors are used to capture the data from hospital environment named heart beat sensor, body temperature sensor, room temperature sensor, CO sensor, and CO_2 sensor. Some more measures which are very significant to determine a patient's condition like the level of diabetes, respiration monitoring, etc. can be addressed as future work.

VIII. REFERENCES

[1]. Z. Zhiao, Chnaowei, and z. Nakdahira,(2013)"Healthcare application based on Internet of Things," in Proc. IEEE Int. Confe. on. Technolgy. Application (pp. 661 662).

[2]. Kortoom, ,Y. Kaiseer, N. Fittop, and D. ramamoorthy, "Canny matters as construction brickss for application of Internet of Things,"IEEE Interne Networks and Comput., vol. 17.

[3]. Z. Achmed and G. Miguel,(2010) "Assimilating Wirel-ess Sensing Nets with Cloud& Computing," 2010 SixtthInnt. Confe. Mobi. Ad-hocc Sense. Netks, (pp. 263–266).

[4]. D. InfanZnta and Hemalattha, "Augmenting Authorisation Construction of Safekeeping with ZIG-BEE using RFID," Vol5, No.4.

[5]. S. M. Riazul Islam, Daehan Kwak, MD. HumaunKabir ,(2015) "The Internet of Things for Health Care: A Comprehensive Survey", DOI 10.1109/ACCESS.2015.2437951.

[6]. Vandana Milind Rohokale, Neeli Rashmi Prasad, Ramjee Prasad, "A Cooperative Internet of Things (IoT) for Rural Healthcare Monitoring and Control",978-1-4577-0787-2/11/ ©2011 IEEE.

[7]. Alexandros Pantelopoulos, Nikolaos G. Bourbakis"A Survey on Wearable Sensor-Based Systems for Health Monitoring and Prognosis",Publisher: IEEE DOI: 10.1109/TSMCC.2009.2032660.

[8]. A.K. Bourke, J.V. O'Brien, G.M. Lyons A.K. Bourke et al.Gait& Posture, (2007)''Evaluation of a threshold-based tri-axial accelerometer fall detection algorithm", (pp.194–199).

[9]. Qiang Li, John A. Stankovic, Mark Hanson, Adam Barth, John Lach, (2009)"Accurate, Fast Fall Detection Using Gyroscopes and Accelerometer Derived Posture Information", DOI: 10.1109/ BSN.2009.46, Sixth International Workshop on Wearable and Implantable Body Sensor Networks, BSN 2009, Berkeley, CA, USA, 3-5.

[10]. J. Chen, K. Kwong, D. Chang (2014)"Wearable Sensors for Reliable Fall Detection", Publisher: IEEE, DOI: 10.1109/IEMBS.2005.1617246. 7. Li Da Xu "A Survey Internet of Things in Industries", IEEE Transactions on Industrial Informatics, Vol. 10, No.4.

[11]. Internet of Things - Architecture (IoT-A). FP7 European Project. Online at: http://www.iot-a.eu/public.

[12]. M. Adnane, Z. Jiang, S. Choi, and H. Jang (2009)"Detecting specific health-related events using an integrated sensor system for vital sign monitoringSensors", 9(9):6897–6912.

[13]. F. Alag¨oz, A. Calero Valdez, W. Wilkowska, M. Ziefle, S. Dorner, and A. Holzinger. ,(2010)From cloud computing to mobile internet, from user focus to culture and hedonism - the crucible of mobile health care and wellness applications. In ICPCA 2010 International Conference on Pervasive Computer Applications, (pp. 1–9).

[14]. J. Blum and E. Magill. M-psychiatry (2008): "Sensor networks for psychiatric health monitoring". In Proceedings of the 9th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting, (pp. 33–37).

[15]. N. Bressan, L. Bazzaco, N. Bui, P. Casari, L. Vangelista, and M. Zorzi (2010)"The Deployment of a Smart Monitoring System Using Wireless Sensor and Actuator Networks". In Proc. of IEEE SmartGridComm, Gaithersburg, MD, USA.