JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SECURE DATA TRANSMISSION IN IOT SMART HEALTHCARE ENVIRONMENT

[1]Sanjeev Kumar, [2]Sukhvinder Singh Deora

[1,2]Department of Computer Science and Application,
Maharshi Dayanand University, Rohtak, India

Abstract : As the use of the Internet of Things (IoT) continues to explode in the field of healthcare, one of the biggest concerns is the safety of patients' personal health information. It is convenient for doctors and patients to use IoT technology in modern hospital environments provides patient monitoring and accurate data management. More opportunities for data security now exist than ever before due to the tremendous improvements in data transmission technology. Existing researchers developed many data protection techniques, including steganography and cryptography. Secure communication between two devices is a challenging issue. In this paper an attempt has been made to propose a secure data transmission framework based on AES in IoT. In proposed mechanism AES of 128bit key is used to generate secret keys for encryption and decryption.

IndexTerms - IoT, Smart Healthcare, IoHT, AES and RSA

I. INTRODUCTION

Rapid advancements in areas such as wireless networking and communication technologies have led to a new paradigm known as the Internet of Things (IoT). According to the IoT, it's possible to provide practically every physical object with an equivalent digital representation [1]. Technologies like RFID and WSN (Wireless Sensor Networking) are only a couple of such examples. Data collected by IoT systems has become a prime target for cybercriminals due to the fact that these systems transmit all of their information from the physical world via the Internet. [2]. Therefore, the data in transit must be protected by using a secure communication channel.

To safeguard the privacy and security of IoHT infrastructure as well as to verify the legitimacy of its users, cryptography is essential. Both symmetric and asymmetric systems exist. However, because of limitations in battery life, processing power, and memory, traditional cryptosystems are ineffective for protecting the IoT. Secure data transmission in IoT networks necessitates the use of efficient, low-weight cryptographic algorithms. Lightweight cryptography ought to be feasible on such devices due to their low power, computational, and memory needs. There needs to be symmetry between security, cost, and performance [3]. To protect sensitive information, cryptography is frequently used [4]. When it comes to digital photographs, there are a number of options for keeping them safe. Using these methods, we can generate random encryption keys while keeping the contents of our data secret [5].

Nowadays, a excess of algorithms utilising a wide variety of cryptographic protocols are used to safeguard sensitive information [6]. When two or more codes are used together, the result is called hybrid encryption [7].The message, a secret manuscript, must be secretly transported into the carrier without being discovered. Capacity and undetectability are two of the most important features of any cryptography system [8]. But it's not easy to find common ground between these two features; increasing capacity in a cryptography system without sacrificing its undetectability is a significant challenge.

This paper is divided into iv sections. In section I introduction of healthcare system and its architecture is presented. Furthermore, cryptography techniques for secure data transmission in IoT has been discussed; section II provides related work of existing techniques; in section III proposed mechanism has been presented in detail; in section IV conclusion of work has been presented.

Contribution:

- This paper provides secure data transmission mechanism for smart healthcare environment.
- The proposed mechanism uses 128-bit AES algorithm for secure data transmission.

II. ARCHITECTURE OF IOHT

Like the IoT design, the IoHT architecture has three levels: the network layer, the perception layer, and the application layer [9]. Figure 1depcits, there are three distinct levels. Medical data and health status information are transmitted from sensors and healthcare device to the cloud via the network layer [10]. This connection can be established via Wi-Fi or other communication sections. Data analysis, monitoring outcomes, reports, and notifications are some of the features provided by healthcare apps, which are useful for doctors, patients, and hospitals. In the worst cases, both patients and doctors can benefit from alerts that come right away as a result of data analytics.

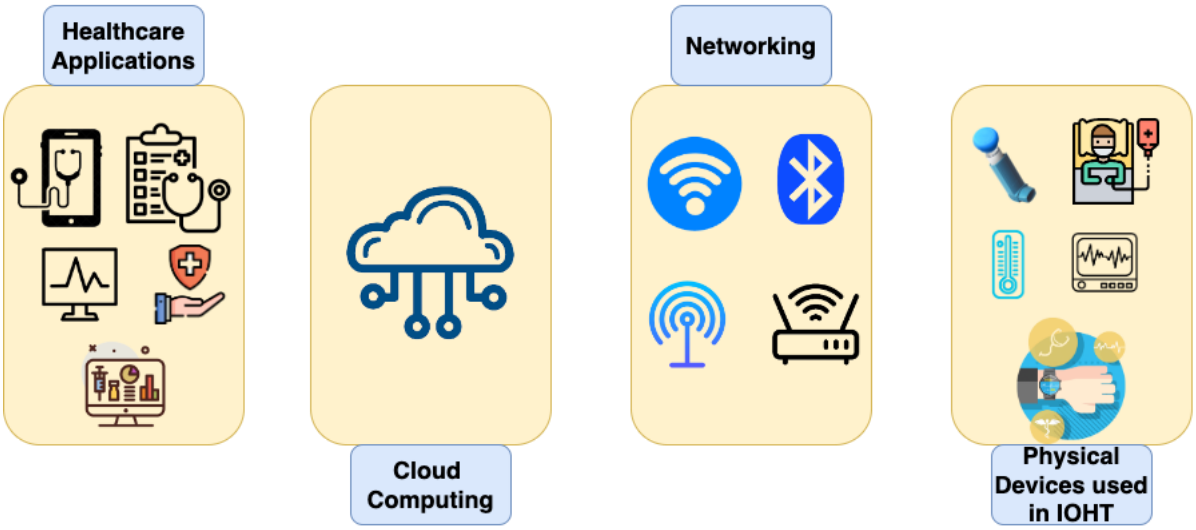

Figure 1 IoT smart healthcare architecture

III. RELATED WORK

Zouka and Hosni [11] suggested integrating artificial intelligence technology like neural networks and fuzzy systems. Similarly, the remedies that need to be implemented, *Karunarathne et al.* [12] Distributed key management was proposed by *Gochhayat et al.* [13] for the IoT ecosystem. By having a local entity handle most of the resource-intensive cryptographic work, the proposed system efficiently delivers security to IoT devices. This entity works with its peers to issue a shared key and verify the authenticity of network devices. The proposed smart healthcare solution for cancer care services draws inspiration from and builds upon the work of *Onasanya and Elshakankiri* [14], who proposed a number of frameworks and architectures to illustrate and support the functional IoT-based solution under consideration or employed in propsoed work. In order to generate keys quickly and securely, *Pirbhulal et al.* [15] created the Triangle Based Security Algorithm (TBSA). For the purpose of eliminating repetition, errors (outliers), and missing values from sensor data, *Sharma et al.* [16] employed a number of preprocessing approaches. The main purpose of this healthcare monitoring system is to find out if something is wrong with a patient's body. If something is wrong, a message is sent to the doctor or emergency centre within one minute. Similarly, *Elhoseny et al.* [17] offer a hybrid security model. The proposed model begins with the encryption of the secret data, with the result hidden in a cover image through 2D-DWT-1L or 2D-DWT-2L. In order to hide the various font sizes, both colour and black-and-white images are utilized as cover images. A secure technique for circular queue data structures was developed by *Albu-Rghaif et al.* [18]. The power of this technique lies in its use of a number of variable parameters that make the original message more difficult to recover by attackers. An improved version of the RECTAN-GLE algorithm, 3D RECTANGLE, was proposed by *Zakaria et al.* [19]. The confusion and diffusion features of the algorithm were enhanced, and the block and key sizes were not increased.
A study was conducted by *Mohammed et al.* [20] to compare different approaches to identifying cyber attacks on the Internet of Things. Furthermore, an overview of IoT integration in healthcare was covered by *Aivaliotis et al.* [21] along with a methodical examination of effective smart health frameworks that rely heavily on a overabundance of devices and sensors that are low on both power and resources. Additionally, a lightweight cryptographic primitive called LEAIoT is used in the proposed lightweight-based security approach. In order to safeguard the diagnostic text information embedded in medical images, *Khan et al.* [22] suggested a hybrid security model. The proposed model is made up of a proposed hybrid encryption system that uses RSA and AES cryptography algorithms.

IV. PROPOSED WORK

In this proposed system, input data consists of 64-bit keys separated into four 16-bit blocks. The 'F' function is then applied to the data blocks. The F function works with 16-bit data. According to the 128-bit AES algorithms, this four-four-bit input data is encoded in matrix form, as described below, and then the X-or operation is used to generate the keys. A new key must be generated for each iteration of the key generation procedure. So that unauthorized individuals cannot access personal or confidential information included within an image. The final generated keys are used to encrypt the data, and the X-or operation is again applied to the final encrypted key. The final key that we receive is also a 64-bit key. The process of keys generation in proposed mechanism is depicted in figure 2.

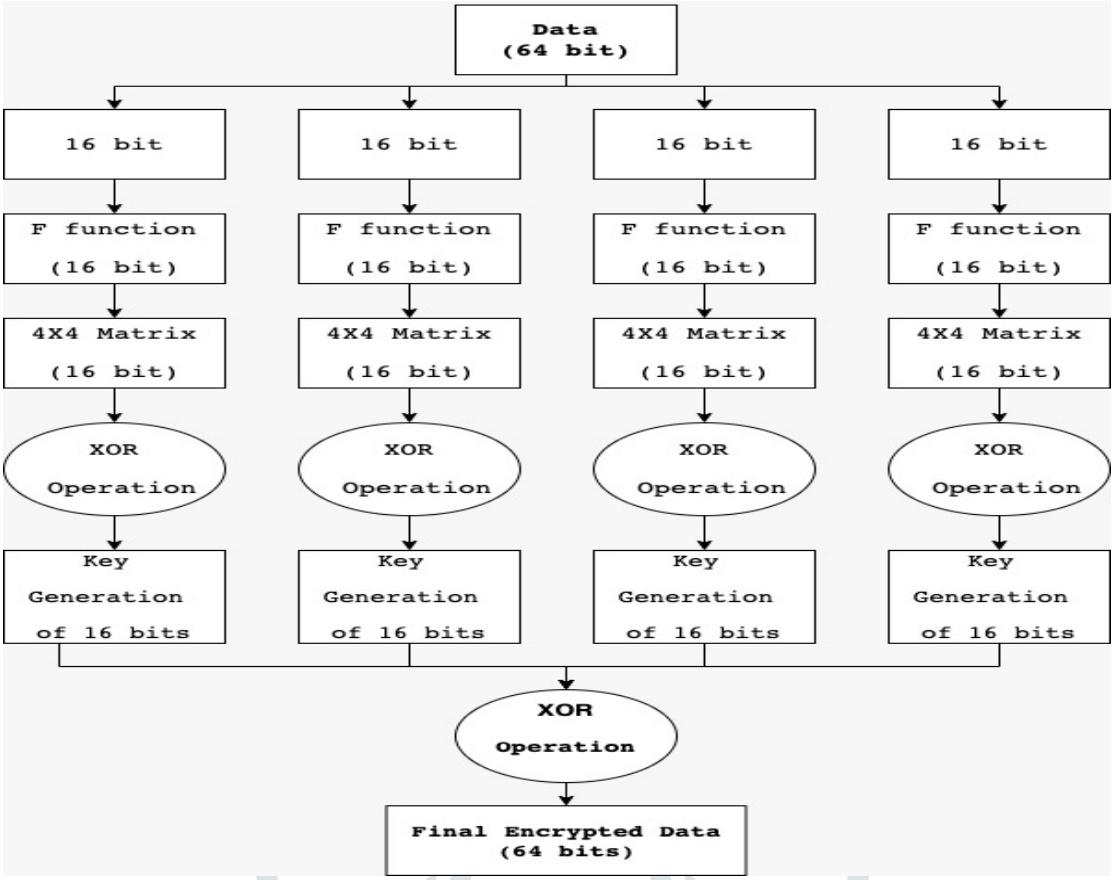

Figure 2 Proposed Framework

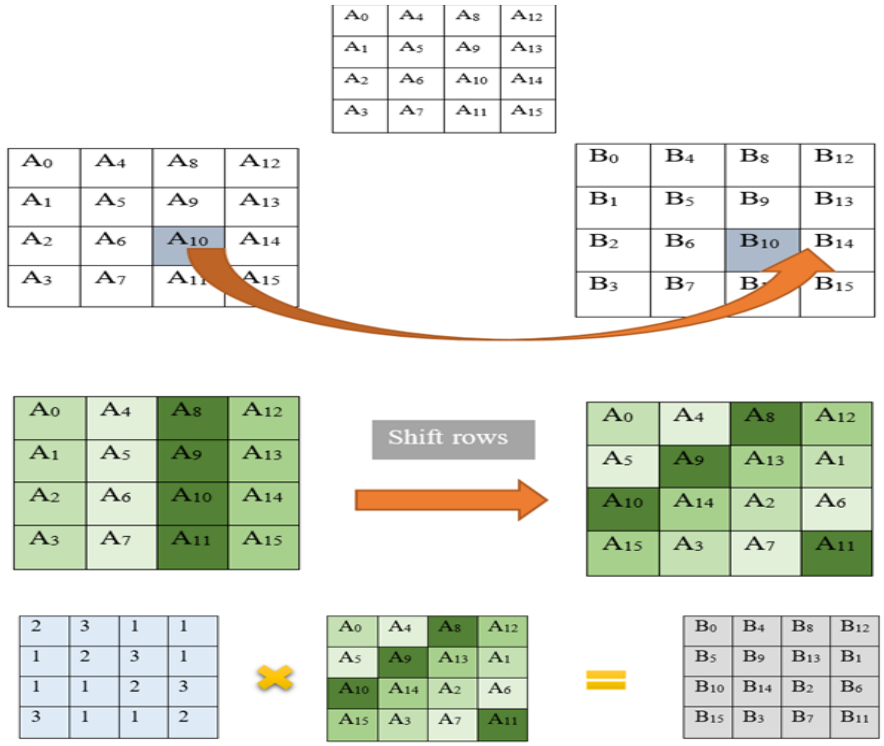

Figure 3 Key Generation Process

For the sake of understanding the AES algorithm, consider a scenario in which 128-bit AES encryption is applied using 10 cycles to complete a round. It employs a 4x4 matrix that represents the 16 bytes, or 0 to 15. When 16 bytes are present, then it can be a matrix of $a_0, a_1 \ldots a_{15}$. Figure 3 depicts the key generation process in detail.

- Shift Rows step: In this step, rows are swapped with one another. The rows are shifted to the left, with the first row remaining intact., the second row shifted by 1, and the nth row shifted by n-1 bytes.

- Mix-Columns step: In this step, four bytes from different columns are joined to form a new column. This is accomplished by multiplying the shift row matrix by the fixed matrix.

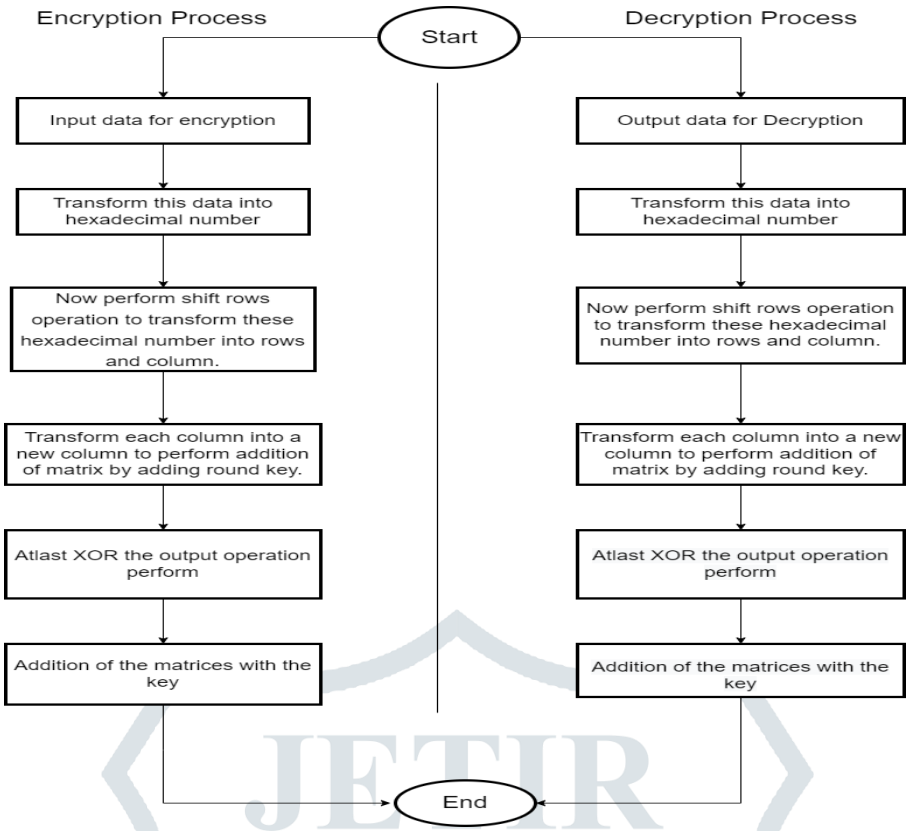

Figure 4 Working of Proposed Framework

The figure 4 depicts the proposed framework. In proposed algorithm for encryption and decryption has been described. When a device in the IoT wants to transmits packets to another device in a safe manner, it first encrypts the message with a private key, which is then decrypted by the receiving device using the same private key. To improve the security of private keys, several rounds will be used to produce them. The AES algorithms process data in the form of bytes. It uses128 bits of a plaintext block as 16 bytes. This block is processed as combination in four columns and four rows. It is dynamic and depends on key length.

V. CONCLUSION

Nowadays, it is difficult to monitor patient health using sensors on their bodies. Sensor nodes can detect heart rate, body temperature, ECG signals, blood pressure, and other parameters. After collecting sensor data, we use pre-processing techniques to eliminate duplication, abnormalities (outliers), and missing values. Transferring information through gateways is a challenging problem. To overcome this problem, in this paper, an AES-based secure data transmission mechanism has been presented. The proposed mechanism uses a 128-bit key for generating the secret key. In future AES can be used to establish secure communication channels and authenticate IoT devices within healthcare networks. Future developments might focus on enhancing device authentication protocols using AES to prevent unauthorized access and data breaches.

REFERENCES

[1] Diwaker, C., Tomar, P., & Sharma, A. 2018. Future aspects and challenges of the internet of things for the smart generation. In Proceedings of International Conference on Communications and Cyber Physical Engineering: 599-606.

[2] Khan, J., Khan, Jhanjhi, M. A., M. Humayun, N. Z., Alourani, A. 2022. Smart-City-based Data Fusion Algorithm for Internet of Things. Comput. Mater. Contin, 73: 2407-2421.

[3] Sharma, R. K., & Nair, A. R. 2019. IoT-based secure healthcare monitoring system. In Proceedings of IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT): 1-6.

[4] Hua, X., Ono, Y., Peng, L., Xu, Y. 2022. Unsupervised Learning Discriminative MIG Detectors in Nonhomogeneous Clutter. IEEE Transactions on Communications, 70(6): 4107-4120.

[5] Liu, J., Sun, S., Liu, W. 2019. One-step persymmetric GLRT for subspace signals. IEEE Transactions on Signal Processing, 67(14): 3639-3648.

[6] Thibaud, M., Chi, H., Zhou, W., Piramuthu, S. 2018. Internet of Things (IoT) in high-risk Environment, Health and Safety (EHS) industries: A comprehensive review. Decision Support Systems, 108: 79-95.

[7] Aftab, H., Gilani, K., Lee, J., Nkenyereye, L., Jeong, S., Song, J. 2020. Analysis of identifiers in IoT platforms. Digital Communications and Networks, 6(3): 333-340.

[8] More, S., Singla, J., Verma, S., Ghosh, U., Rodrigues, J. J., Hosen, A. S., Ra, I. H. 2020. Security assured CNN-based model for reconstruction of medical images on the internet of healthcare things. IEEE Access, 8: 126333-126346.

[9] Shankar, K., Lakshmanaprabu, S. K. 2018. Optimal key based homomorphic encryption for color image security aid of ant lion optimization algorithm. International Journal of Engineering & Technology, 7(9): 22-27.

[10] Rani, S. S., Alzubi, J. A., Lakshmanaprabu, S. K., Gupta, D., Manikandan, R. 2020. Optimal users based secure data transmission on the internet of healthcare things (IoHT) with lightweight block ciphers. Multimedia Tools and Applications, 79(47): 35405-35424.

[11] El Zouka, H. A., Hosni, M. M. (2021). Secure IoT communications for smart healthcare monitoring system. Internet of Things, 13: 1-14.
[12] Karunarathne, S. M., Saxena, N., Khan, M. K. 2021. Security and privacy in IoT smart healthcare. IEEE Internet Computing, 25(4): 37-48.
[13] Gochhayat, S. P., Lal, C., Sharma, L., Sharma, D. P., Gupta, D., Saucedo, J. A. M., Kose, U. 2020. Reliable and secure data transfer in IoT networks. Wireless Networks, 26(8): 5689-5702.
[14] Onasanya, A., Elshakankiri, M. 2021. Smart integrated IoT healthcare system for cancer care. Wireless Networks, 27(6): 4297-4312.
[15] Pirbhulal, S., Zhang, H., E Alahi, M. E., Ghayvat, H., Mukhopadhyay, S. C., Zhang, Y. T., Wu, W. 2016. A novel secure IoT-based smart home automation system using a wireless sensor network. Sensors, 17(1): 1-19.
[16] Sharma, R. K., Nair, A. R. 2019. Iot-based secure healthcare monitoring system. In Proceedings of IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT): pp. 1-6.
[17] Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O. M., Shawkat, S. A., Arunkumar, N., Farouk, A. 2018. Secure medical data transmission model for IoT-based healthcare systems. IEEEE Access, 6: 20596-20608.
[18] Albu-Rghaif, A. N., Jassim, A. K., Abboud, A. J. 2018. A data structure encryption algorithm based on circular queue to enhance data security. In Proceedings of 1st International Scientific Conference of Engineering Sciences-3rd Scientific Conference of Engineering Science (ISCES): 24-29.
[19] Zakaria, A. A., Azni, A. H., Ridzuan, F., Zakaria, N. H., Daud, M. 2020. Extended RECTANGLE algorithm using 3D bit rotation to propose a new lightweight block cipher for IoT. IEEE Access, 8: 198646-198658.
[20] K. Mohammed, A. H., Jebamikyous, H., Nawara, D., & Kashef, R. 2021. Iot cyber-attack detection: A comparative analysis. In Proceedings of International Conference on Data Science, E-learning and Information Systems: 117-123.
[21] Aivaliotis, V., Tsantikidou, K., Sklavos, N. 2022. IoT-Based Multi-Sensor Healthcare Architectures and a Lightweight-Based Privacy Scheme. Sensors, 22 (11): 1-21.
[22] Khan, M. A., Khan, J., Sehito, N., Mahmood, K., Ali, H., Bari, I., Ghoniem, R. M. 2022. An Adaptive Enhanced Technique for Locked Target Detection and Data Transmission over Internet of Healthcare Things. Electronics, 11(17): 1-17.