Securing Physiological Signals and Patient ID using Multilayer Encryption and Scattered Steganography

Adarsha Bhattarai
Department of *Electrical and Computer Engineering*
University of Nebraska-Lincoln
Omaha, USA
abhattarai3@huskers.unl.edu

Abstract—**Remote monitoring of the patients in a distributed network can be vulnerable to attackers. It needs more attention in terms of the confidentiality of the patient's physiological signal and identity. This project presents the combination of AES encryption and scattered steganography to secure the physiological signals and ensure the patient's anonymity. Scattered steganography is very efficient and adds extra protection from attackers and intruders. The attacker is unaware of the fact that the ECG signal itself represents the identity of the patient. The robustness of the proposed combination of encryption and steganography is validated by recovering transmitted ECG signals even in very low SNR conditions.**

Keywords—AES Encryption, Distributed network, Steganography

I. Introduction

A. Background

With the advancement of technologies, the Internet of Medical Things (IoMT) has transformed the traditional healthcare system to a new level. It is expected that by 2027 Internet of Medical Things market would reach up to $ 284.5 billion worldwide [1]. The availability of resources such as high-speed internet, 4G and 5G cellular networks, Bluetooth, Wi-Fi, cloud services, small but powerful embedded systems, and powerful processing platforms have led to the rapidly growing telemedicine industry. However, along with this growth, there come plenty of challenges concerning the management of processing layers, vulnerabilities in data transmission, communication costs, and delays [2-23].

In the future, with the present infrastructure, the increasing number of IoMT users could bring many complexities to the network like security threats, high data traffic, and signal degradation that might affect the real-time diagnosis. Many researchers have suggested moving towards distributed network rather than a centralized cloud system [11-18]. This could not only save the transmission energy but also reduce exposure to hackers and intruders.

Access to powerful cloud servers and edge computing has improved the remote diagnosis of the patient. However, IoMT devices are still vulnerable to attackers. In addition to wearable ECG sensors, implantable devices like cardiac pacemakers, cardioverter defibrillators, insulin pumps, and neurostimulators have serious security threats [3-5]. Various threats like data leaks, distributed denial-of-service (DDoS), Man-in-the-middle attacks (MITM), etc. have been recorded in recent years [3-10]. Risk factors concerning data leaks, data stealing, data modification, and unauthorized access could happen during data collection by the local layer, data transmission between layers, and data storage. A system covering the security measures for such threats in multiple processing layers i.e., local, edge/fog, and cloud layer is a prerequisite for a safe and sound telemedicine application. Therefore, confidentiality, integrity, availability, nonrepudiation, and authentication together termed CIANA is essential for secure IoMT applications [2].

According to a recent study, it is calculated that the IoMT healthcare system could save $ 3000 billion in expenses every year [1]. So, the design of the secured collaborative infrastructure for the local, edge/fog, and medical layers could be worth the investment which could reduce the overall expenses while improving patient care. To develop an IoMT system that is resistant to cyber threats, researchers have proposed many cryptography and steganography techniques or a combination of these techniques. [20-33]. I believe along with these types of security solutions it is also necessary to research the challenges that might arrive while applying such algorithms on various processing nodes. The local sensor node is resource-constraint in terms of processing power and battery power. Hence, the security algorithm proposed for such devices should be very efficient and at the same time secured.

B. Overview of the work

This project is focused on the confidentiality of the transmitted medical data and patient information in the IoMT network. Most importantly the patient's identity is given more priority in terms of confidentiality. A combination of encryption and steganography is proposed to secure patient information and other medical data. Steganography is responsible for securing patients' identities while encryption protects other medical data. The proposed scattered steganography is blended with symmetric cryptography, Advanced Encryption Standard (AES) to transmit data from the local layer to the medical server in a secured environment. The proposed scattered steganography uses the physiological signal of the patient to secure the information. It is embedding less steganography and hence is very efficient. This approach will help the resource-constraint embedded systems to accommodate the proposed hybrid algorithm efficiently. When the patient's identity is secured by the scattered steganography there is a lesser chance the attacker will find out about the owner of the physiological signal even if the physiological signal is compromised. This is less damaging when the attacker is unaware of whose medical data it is. This project uses ECG signals acquired from the MIT-BIH Arrhythmia Database for the implementation of the proposed hybrid algorithm and analysis.

II. LITERATURE REVIEW

Ogundokun et al. proposed a combination of steganography and cryptography methods to secure medical data in the IoMT network [27]. They used International Data Encryption Algorithm (IDEA) for the encryption of medical data initially and finally used Matrix-XOR to embed encrypted information to an external cover object. Gull et. al. put forward the idea of using two images as cover objects to embed the patient information that was initially encrypted using Huffman encoding [28]. This increased the overall embedding capacity and improved the SNR. However, these papers lacked the idea of the implementation of the proposed technique in real-time medical analysis. The medical data could be a continuous signal generated from the local device. If they use the same cover image multiple times, it might be the point of vulnerability and if they use multiple cover images, it might increase the time required for the encryption and embedding. I believe that when the combination of steganography and cryptography is used, a medical signal or image by itself could be implemented as a cover image resulting in a more efficient algorithm.

Unlike Ogundokun et al. [27] and Gull et al. [28], Devi et al. [31] used the MR image of the brain itself as the cover image to hide patient information using LSB steganography. They even validated the use of Computer-Aided Diagnosis (CAD) on the formed stego images. However, their security model did not discuss any cryptography methods for encrypting the formed stego images for the more secure transmission of the data in the network. Encryption after embedding the patient identity to the cover object would have contributed to the robustness of the proposed technique.

Pirbhulal et al. proposed bio-keys extracted from the ECG signals based on the R-peak detection algorithm [24]. The key they developed was extracted from the patient's ECG signal at a particular instance. Since the ECG signal is changing every time the key-value might also differ from time to time for each patient. Multiple-key management could be a challenge in the proposed IoMT application.

III. SYSTEM ARCHITECTURE

The proposed system architecture consists of an attacker and security measures applied to the local ECG sensor, edge layer, and medical server. Advanced Encryption Standard (AES) scattered steganography is applied to transmit the ECG signal and patient information securely from one processing node to another. The processing nodes refer to the three major layers local, edge, and medial layers. The layers proposed in the system and the technique used is explained in the following section.

Local Layer: This layer consists of the ECG sensor and embedded system with limited processing power. The initial diagnosis of the ECG signal is conducted here. The patient ID is safely encrypted and then scattered steganography is performed on the ECG signal before the transmission to other layers.

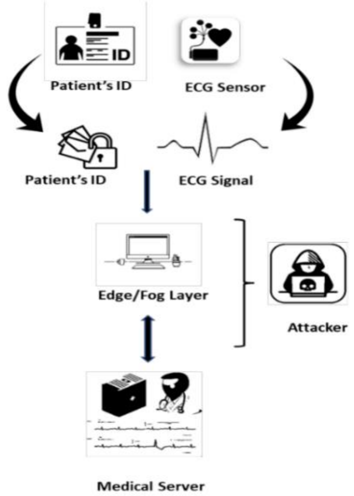

Fig 1. Proposed System Architecture

Edge layer: The edge device might be a modern smartphone or a laptop which is more powerful than a local device. After the initial ECG diagnosis, the results reported by the local device are reverified by the edge device. Later, all the collected data by the edge layer is transmitted to the medical layer.

Medical layer: This layer receives all the diagnosis reports from other layers. ECG signals of the patient and other medical data are received in encrypted form. Decryptions and stego analysis are needed to decipher all the information. Finally, the patient will undergo treatment according to their needs.

Attacker: The attacker lies between the local ECG sensor and the medical server and tries to steal the medical data that is transmitted from one layer to another. The attacker uses various methods to steal medical data like man-in-the-middle (MITM) attacks. The MITM is performed by deploying the rogue access point into the area of medical institutions and trying to penetrate the network.

Advanced Encryption Standard (AES): Proposed remote diagnosis system uses AES 128-bit encryption as the cryptography tool to encrypt patient information. Since the input size of the used AES encryption is 128 bits, the patient information is divided into blocks of 128 bits. Then these blocks are encrypted with the 256-bit key and ready to be hidden inside the ECG signals following the scattered steganography algorithm.

Scattered Steganography: After the patient information and diagnosis results obtained from the local or edge layers are encrypted using the AES algorithm, they get ready for scattered steganography. The idea behind the proposed novel scattered steganography is that each ECG samples are unique and represent a unique binary feature. The two types of binary identity as even and odd parity ECG samples are categorized. These features of the ECG samples are used to represent the personal information of the patient in the ECG signal. The locations of the ECG samples that represent the secret patient identity are pseudo-randomly selected by the scattered stego algorithm.

If the attacker somehow gets access to the transmitted ECG signals, they might read the ECG signal but will not be aware that the random ECG samples itself in the ECG signal are representing the patient's identity. This will ensure the anonymity of the patient even when their ECG signals are stolen and are less damaging.

IV. METHODOLOGICAL FRAMEWORK

In the proposed IoMT system, the AES encryption and the scattered steganography are deployed on all processing nodes. These two techniques are responsible for securing the patient’s personal information and the physiological signal at each node of a distributed system.

A. Encryption

In the local layer, the initial diagnosis occurs with an efficient diagnosis algorithm. Then the initial diagnosis reports are created at this layer. These reports along with the patient’s personal information are encrypted using AES. The input to the AES algorithm is a block of length 128-bits. Hence, the reports and patient identity must be converted to multiple blocks of 128 bits. About the key, either the 128-bit key or the 256-bit key could be used to convert the plain input block into the ciphertext. KEY-1 is used as 256-bit key. Algorithm 1 shows the step-by-step process of encryption.

Algorithm 1: Encrypt the patient’s identity

Input:	Patient ID and ECG signals *ecg(t)* of the patient.
Output:	Encrypted Patient ID which is made ready to be embedded inside the *ecg(t)*
Step 1:	Calculate the hexadecimal value of the Patient ID
Step 2:	Resize each input block to 128 bit and get ready for encryption
Step 3:	Encrypt the value of step 2 using 256-bit KEY and AES 128-bit encryption
Step 4:	Acquire the *ecg(t)* of the patient and the encrypted patient ID
Step 5:	Get ready for the scattered steganography

C. Parity check of the ECG signal

After the encryption is carried out each ECG sample of the patient is evaluated to find the parity status. The location of every even and odd parity ECG sample is recorded before the mapping is performed between the binary bits of patient identity and ECG samples. The encrypted patient identity is mapped to the ECG signal by the pseudo-randomly generated location referred to as KEY-2. The following algorithm explain the procedure involved in the scattered steganography.

Algorithm 2: Scattered Steganography

Input:	Encrypted patient ID and ECG signals *ecg(t)* of the patient.
Output:	ECG signal ecg*(t)* embedded with Encrypted Patient ID
Step 1:	Convert both the *ecg(t)* signal and patient ID to the binary form
Step 2:	Find the parity of *ecg(t)* signal samples and mark the odd or even parity of each sample
Step 3:	Generate a random mapping of each binary bits of patient identity to the odd or even parity of *ecg(t)*
Step 4:	Patient ID is represented by random ECG samples in the *ecg(t)* and save the location as KEY 2

F. Decryption, stego analaysis and treatment

The final comprehensive diagnosis is carried out in the medical layer where the cardiologists review the patient case and start the treatment as soon as necessary. Once the diagnosis results and the patient’s data reach the medical layer from the local layer and edge layer they go under the decryption and stego analysis process. Three keys are involved in the process until the ECG signal, diagnosis reports, and patient identity are extracted. The following algorithm summarizes the steps involved.

Algorithm 3: Decryption and stego analysis

Input:	ECG signals *ecg(t)* from the edge layer embedded with encrypted patient ID and diagnosis results
Output:	Decryption results of the patient’s ID and verification of the diagnosis results from the edge/fog layer
Step 1:	Using KEY-3 decrypt stego *ecg(t)* signals in which the patient’s ID is embedded.
Step 2:	Using KEY-2 find the scattered location of all *n* samples of stego *ecg(t)* signals which represent the patient’s ID
Step 3:	Decrypt the encrypted binary Patient ID using AES 128-bit input and 256-bit KEY-1
Step 4:	Perform the analysis of ECG data by the professionals

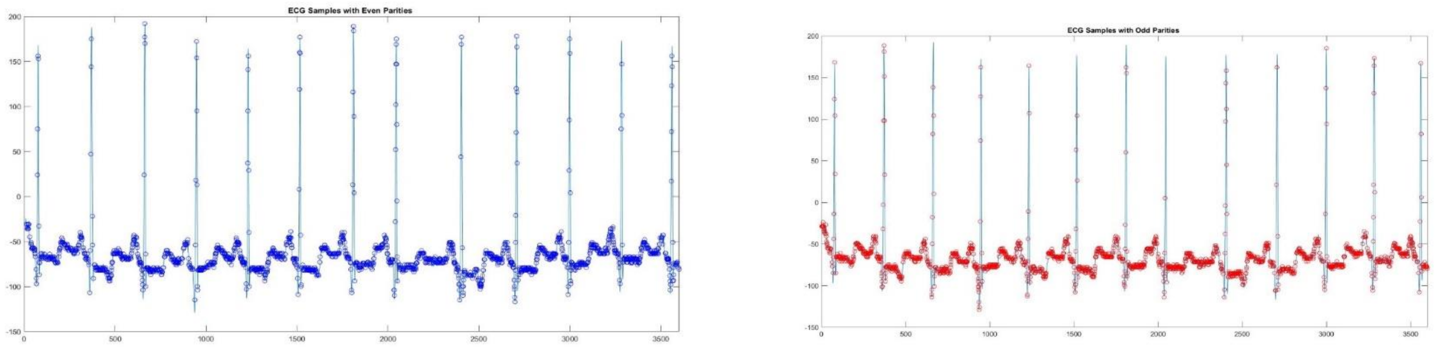

Fig 2. Searching and locating ECG samples with even parities(left) and odd parities(right)

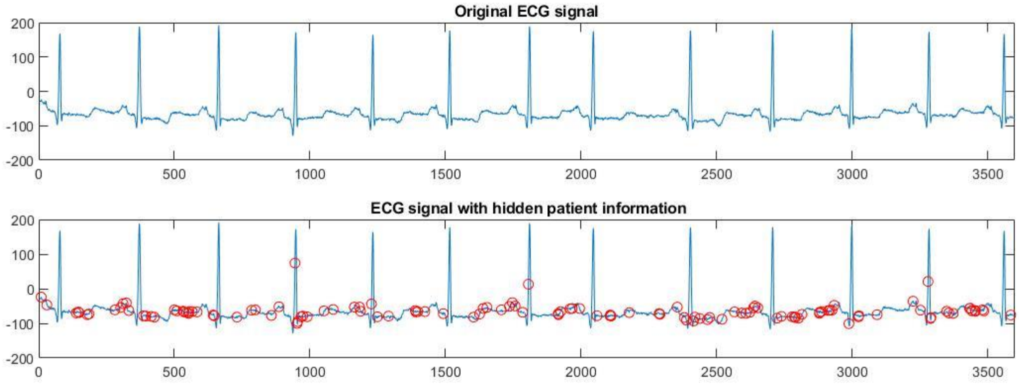

Fig 3. Mapping of 128-bit patient identity to their ECG signal

V. SIMULATION

The simulations were performed using MATLAB 2020b. Datasets used in the simulations are obtained from the MIT-BIH Arrhythmia Database [34-35]. The simulation tasks are divided into the following subsections.

A. Encryption of patient identity and ECG data

The patient ID was converted into 128 bits as the necessary input size for AES 128-bit. Zero padding was performed to make the desired length. Finally, the patient ID was encrypted using AES with a 256-bit key.

Table 1 Encryption of Patient ID

Patient ID	**'30735 '**
Encrypted Patient ID	'÷lâz¿Z+ð9[ÄÐ? '

B. Scattered Steganography

After the encryption of the patient ID, scattered steganography was performed. 128 bits of patient ID were mapped to pseudo-randomly generated ECG samples based on their parity status. Before the mapping, the parity status of each ECG sample was recorded as shown in figure 2. Finally, the mapping of 128 bits of patient identity was mapped to the ECG signal as shown in figure 3.

C. Scattered Steganography Under Gaussian Noise

To test the performance of the proposed scattered steganography, additive white gaussian noise (AWGN) was introduced to the channel after the modulation process [36]. As a widely used digital modulation, 16 QAM was used to modulate the encrypted ECG signal that represented the patient ID. The AWGN was applied for various transmitted

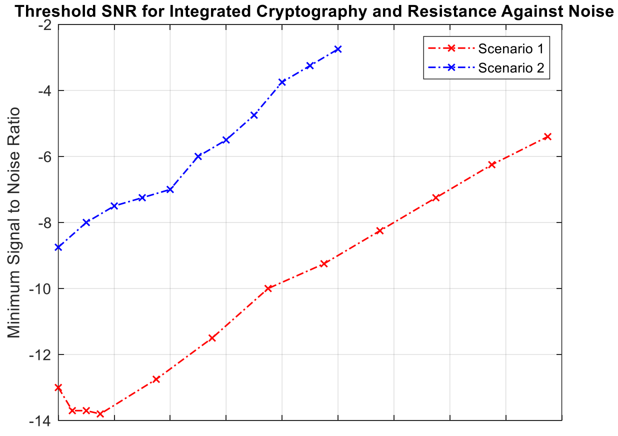

Fig 4. Scattered Steganography in the Presence of Gaussian Noise and Range Validation for Various Signal Powers

signals with power ranging from 0 dbW to 5 dbW. After that, the minimum required SNR values to perform the stego-analysis successfully at the receiver end were obtained for every transmitted signal.

Again, a similar experiment was repeated for the transmitted signals with the power ranging from 0 dbW to 9 dbW. Then the respective minimum required SNR values to perform the stego-analysis successfully at the receiver side were obtained for all transmitted signals. The proposed scattered steganography was robust to every SNR value that was greater than or equal to the calculated threshold SNR values for both experiments.

The graph in figure 4 represents the threshold SNR values for two sets of experiments with transmitted signal power ranging from 0 dbW to 5 dbW and 0 dbW to 9 dbW respectively. These experiments demonstrated that the proposed steganography was resistant to such a low SNR condition.

D. Discussion on Security Services

This project is mainly focused on the confidentiality of the medical data and the anonymity of the patient's identity. The other security services like authentication, authorization, and integrity are beyond the scope of this project. However, the future direction of this project heads to the application of medical blockchain. This would allow an opportunity to address the security services like authentication and authorization of processing layers, medical staff, etc.

VI. CONCLUSION

The hybrid security mechanism was proposed for the medical application. It consisted of multiple AES encryption and scattered steganography. The project mainly focused on the confidentiality of the medical data and the anonymity of the patient. Scattered steganography contributed to the anonymity of the patient's identity. Even the attacker is unaware of the presence of patient identity that is mapped to the ECG signal. The robustness of the scattered steganography was validated by applying white noise to the transmitted ECG signal and then recovering the ECG data back even in low SNR conditions. The future direction of the project would be the inclusion of a medical blockchain to authenticate and authorize various processing nodes to access services and resources.

REFERENCES

[1] https://www.prnewswire.com/in/news-releases/internet-of-medical-things-market-to-reach-us-284-5-billion-by-2027-globally-cagr-18-5-univdatos-market-insights-850218832.html

[2] Ghubaish, Ali, Tara Salman, Maede Zolanvari, Devrim Unal, Abdulla Khalid Al-Ali, and Raj Jain. "Recent advances in the internet of medical things (iomt) systems security." *IEEE Internet of Things Journal* (2020).

[3] Hassija, Vikas, Vinay Chamola, Balindam Chandra Bajpai, and Sherali Zeadally. "Security issues in implantable medical devices: Fact or fiction?." Sustainable Cities and Society 66 (2021): 102552.

[4] Camara, C., Peris-Lopez, P., De Fuentes, J.M. and Marchal, S., 2020. Access control for implantable medical devices. IEEE Transactions on Emerging Topics in Computing.

[5] Puat, H.A.M. and Abd Rahman, N.A., 2020, December. IoMT: A Review of Pacemaker Vulnerabilities and Security Strategy. In Journal of Physics: Conference Series (Vol. 1712, No. 1, p. 012009). IOP Publishing.

[6] Khan, M.A., Quasim, M.T., Alghamdi, N.S. and Khan, M.Y., 2020. A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data. IEEE Access, 8, pp.52018-52027.

[7] Cope, Peter, Joseph Campbell, and Thaier Hayajneh. "An investigation of Bluetooth security vulnerabilities." In 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), pp. 1-7. IEEE, 2017.

[8] Sevier, Seth, and Ali Tekeoglu. "Analyzing the security of Bluetooth low energy." In *2019 International Conference on Electronics, Information, and Communication (ICEIC)*, pp. 1-5. IEEE, 2019.

[9] Hassan, Shaikh Shahriar, Soumik Das Bibon, Md Shohrab Hossain, and Mohammed Atiquzzaman. "Security threats in Bluetooth technology." *Computers & Security* 74 (2018): 308-322.

[10] Lonzetta, Angela M., Peter Cope, Joseph Campbell, Bassam J. Mohd, and Thaier Hayajneh. "Security vulnerabilities in Bluetooth technology as used in IoT." *Journal of Sensor and Actuator Networks* 7, no. 3 (2018): 28.

[11] Greco, Luca, Gennaro Percannella, Pierluigi Ritrovato, Francesco Tortorella, and Mario Vento. "Trends in IoT based solutions for health care: Moving AI to the edge." Pattern recognition letters 135 (2020): 346-353.

[12] Mutlag, Ammar Awad, Mohd Khanapi Abd Ghani, Mazin Abed Mohammed, Abdullah Lakhan, Othman Mohd, Karrar Hameed Abdulkareem, and Begonya Garcia-Zapirain. "Multi-Agent Systems in Fog–Cloud Computing for Critical Healthcare Task Management Model (CHTM) Used for ECG Monitoring." *Sensors 21*, no. 20 (2021): 6923.

[13] Tuli, Shreshth, Nipam Basumatary, Sukhpal Singh Gill, Mohsen Kahani, Rajesh Chand Arya, Gurpreet Singh Wander, and Rajkumar Buyya. "HealthFog: An ensemble deep learning based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments." *Future Generation Computer Systems* 104 (2020): 187-200.

[14] Farahani, Bahar, Mojtaba Barzegari, Fereidoon Shams Aliee, and Khaja Ahmad Shaik. "Towards collaborative intelligent IoT eHealth: From device to fog, and cloud." *Microprocessors and Microsystems* 72 (2020): 102938.

[15] Rincon, Jaime A., Solanye Guerra-Ojeda, Carlos Carrascosa, and Vicente Julian. "An IoT and Fog Computing-Based Monitoring System for Cardiovascular Patients with Automatic ECG Classification Using Deep Neural Networks.*" Sensors 20,* no. 24 (2020): 7353.

[16] Gill, Sukhpal Singh, Rajesh Chand Arya, Gurpreet Singh Wander, and Rajkumar Buyya. "Fog-based smart healthcare as a big data and cloud service for heart patients using IoT." *In International Conference on Intelligent Data Communication Technologies and Internet of Things*, pp. 1376-1383. Springer, Cham, 2018.

[17] Moghadas, Ehsan, Javad Rezazadeh, and Reza Farahbakhsh. "An IoT patient monitoring based on fog computing and data mining: Cardiac arrhythmia usecase." *Internet of Things 11* (2020): 100251.

[18] Djelouat, Hamza, Mohamed Al Disi, Issam Boukhenoufa, Abbes Amira, Faycal Bensaali, Christos Kotronis, Elena Politi, Mara Nikolaidou, and George Dimitrakopoulos. "Real-time ECG monitoring using compressive sensing on a heterogeneous multicore edge-device." *Microprocessors and Microsystems 72* (2020): 102839.

[19] Cheikhrouhou, Omar, Redowan Mahmud, Ramzi Zouari, Muhammad Ibrahim, Atef Zaguia, and Tuan Nguyen Gia. "One-dimensional CNN approach for ECG arrhythmia analysis in fog-cloud environments." *IEEE Access 9* (2021): 103513-103523

[20] Sahu, Neerja, Dongming Peng, and Hamid Sharif. "Diagnosis-Steganography-Transmission: An Innovative Integrated Paradigm for ECG Healthcare." *SN Computer Science 2*, no. 4 (2021): 1-22.

[21] Sahu, Neerja, Dongming Peng, and Hamid Sharif. "An innovative approach to integrate unequal protection-based steganography and progressive transmission of physiological data." *SN Applied Sciences 2*, no. 2 (2020): 1-23.

[22] Sahu, Neerja, Dongming Peng, and Hamid Sharif. "Joint steganography-source-channel coding for wireless physiological signal transmission." *In 2018 IEEE International Conference on Communications (ICC)*, pp. 1-6. IEEE, 2018.

[23] Sahu, Neerja, Dongming Peng, and Hamid Sharif. "Unequal steganography with unequal error protection for wireless physiological signal transmission." *In 2017 IEEE International Conference on Communications (ICC)*, pp. 1-6. IEEE, 2017

[24] Pirbhulal, Sandeep, Oluwarotimi Williams Samuel, Wanqing Wu, Arun Kumar Sangaiah, and Guanglin Li. "A joint resource-aware and medical data security framework for wearable healthcare systems." *Future Generation Computer Systems 95* (2019): 382-391.

[25] Janveja, Meenali, Bikram Paul, Gaurav Trivedi, Gonella Vijayakanthi, Astha Agrawal, Pidanič Jan, and Zdeněk Němec. "Design of Efficient AES Architecture for Secure ECG Signal Transmission for Low-power IoT Applications." *In 2020 30th International Conference Radioelektronika* (RADIOELEKTRONIKA), pp. 1-6. IEEE, 2020.

[26] Shaikh, Muhammad Umair, Siti Anom Ahmad, and Wan Azizun Wan Adnan. "Investigation of data encryption algorithm for secured transmission of electrocardiograph (ECG) signal*." In 2018 IEEE-EMBS Conference on Biomedical Engineering and Sciences (IECBES)*, pp. 274-278. IEEE, 2018.

[27] Ogundokun, Roseline Oluwaseun, Joseph Bamidele Awotunde, Emmanuel Abidemi Adeniyi, and Femi Emmanuel Ayo. "Crypto-Stegno based model for securing medical information on IOMT platform." *Multimedia tools and applications 80*, no. 21 (2021): 31705-31727.

[28] Gull, Solihah, Shabir A. Parah, and Khan Muhammad. "Reversible data hiding exploiting Huffman encoding with dual images for IoMT based healthcare." *Computer Communications 163* (2020): 134-149.

[29] ALRikabi, Haider TH, and Hussein Tuama Hazim. "Enhanced Data Security of Communication System Using Combined Encryption and Steganography." *International Journal of Interactive Mobile Technologies 15*, no. 16 (2021).

[30] Khan, Muhammad Farrukh, Taher M. Ghazal, Raed A. Said, Areej Fatima, Sagheer Abbas, M. A. Khan, Ghassan F. Issa, Munir Ahmad, and Muhammad Adnan Khan. "An IoMT-Enabled Smart Healthcare Model to Monitor Elderly People Using Machine Learning Technique." *Computational Intelligence and Neuroscience 2021* (2021).

[31] Devi, Swagatika, Manmath Narayan Sahoo, Khan Muhammad, Weiping Ding, and Sambit Bakshi. "Hiding medical information in brain MR images without affecting accuracy of classifying pathological brain." *Future Generation Computer Systems* 99 (2019): 235-246.

[32] Elhoseny, Mohamed, K. Shankar, S. K. Lakshmanaprabu, Andino Maseleno, and N. Arunkumar. "Hybrid optimization with cryptography encryption for medical image security in Internet of Things." *Neural computing and applications* (2018): 1-15.

[33] Ibaida, Ayman, Alsharif Abuadbba, and Naveen Chilamkurti. "Privacy-preserving compression model for efficient IoMT ECG sharing." *Computer Communications* 166 (2021): 1-8.

[34] Moody GB, Mark RG. The impact of the MIT-BIH arrhythmia database. IEEE Eng Med Biol Mag [Internet]. 2001 May;20(3):45–50. Available from: http://dx.doi.org/10.1109/51.932724

[35] Goldberger AL, Amaral LA, Glass L, Hausdorff JM, Ivanov PC, Mark RG, et al. PhysioBank, PhysioToolkit, and PhysioNet: components of a new research resource for complex physiologic signals. Circulation [Internet]. 2000 Jun 13;101(23):E215-20. Available from: http://dx.doi.org/10.1161/01.cir.101.23.e215

[36] Add white Gaussian noise to signal - MATLAB awgn [Internet]. . Available from: https://www.mathworks.com/help/comm/ref/awgn.html