Al-Qadisiyah Journal of Pure Science

Volume 29 | Number 2 Article 19

12-20-2024

Secure Data Transmission in Multi-PAN Network Enhanced by AI

Esraa Raheem Alzaidi
College of Since, University of Al-Qadisiyah, Al-Qadisiyah, Iraq, esraa.alzaidi@qu.edu.iq

ORIGINAL STUDY

Secure Data Transmission in Multi-PAN Network Enhanced by AI

Esraa R. Alzaidi

College of Since, University of Al-Qadisiyah, Al-Qadisiyah, Iraq

Abstract

In WMSN, sensors that can be worn or put inside the body, collect information about a patient's health. These details are saved in a database at the hospital. Someone who wants to harm can make it difficult to communicate by blocking messages or change the messages. There may be a problem. In this project, we protect the database using special methods and control who can access certain data. We suggest using AI enhancement to make things more secure in our project. This prevents the patient's information from being changed.

Keywords: Data transmission, Multi-PAN, Enhancing, AI

1. Introduction

In simple terms: Recently, there has been fast progress in making wearable biosensor devices and wireless communication technologies. This has led to the creation of wireless medical sensor networks (MSNs) which are very promising. These networks will bring big changes to how healthcare is obtained, whether at home, in hospitals, or in large medical facilities. Instead of checking patients' health in person, their health measurements can now be monitored from a distance in real-time. The data can be processed and sent to medical databases. This medical information is shared with and used by different people like healthcare workers, researchers, government organizations, insurance companies, and patients. This method will make healthcare faster and easier, helping with things like diagnosing illnesses and responding to emergencies. It will greatly improve how well healthcare works [1].

A really big MSN can have tens of smaller networks for patients to use and, each PAN has many biosensor nodes which is used for security. The database is protected by techniques and controlled data access in the project. For our project, we suggest using Symmetric key encryption/decryption to increase security [2].

This keeps patient information from being changed and handles the process of verifying the identity of users accessing medical information. We conduct this to make sure that the right people can access important medical information and prevent attacker's access. Additionally, the information gathered from a biosensor is sent to the controller in clear text. This means nor anybody can change or add undesired information to the medical records that are stored on the computer network. Some scientists use the signals given by a patient's body, like heart rate and blood levels, to help a device create a secret code that both parties can agree on and use securely. They want each biosensor to measure only one thing, but this limits its usefulness for different uses [3].

2. Literature review

In terms of methods that are applied, there are two methods: Code Blue and Alarm-Net where Code Blue combines different devices that use wireless technology in a situation where there is a disaster. It allows these devices to connect and work together. It also has features to help keep the information flowing safely and freely, and to group the information produced by the sensors. Benefits of

Received 30 June 2023; accepted 24 March 2024.
Available online 18 April 2025
E-mail address: Esraa.alzaidi@qu.edu.iq.

https://doi.org/10.29350/2411-3514.1299

using RF technology to track the location of something or someone [1,4].

There are problems with medical sensor networks because they take too long to compute and cannot meet strict timing needs. These security methods are not strong enough to prevent Denial-of-Service attacks [2].

The second method is Alarm-Net, healthcare apps are seen as good opportunities for development. Wireless devices can be used to check on patients. We use WMSNs to create networks of medical sensors that work without wires. Alarm-Net is meant to monitor the health of patients, helpful for places to live and staying home. Advantage-Alarm-Net helps keep networks and data safe for people who live in physiological places for example. Monitoring and listening to patient's vital signs can have negative effects. Monitoring symbols or indications and keeping an eye on what you do and where you are can be dangerous [5].

3. Existing system

Wireless medical sensor networks (MSNs) help in many medical practices. Technology used in electronic healthcare that collects information about a patient's health where important body measurements that can be gathered by wearable devices. Tiny medical sensors that can be inserted into the body. However, keeping things secret and keeping the information safe is a big problem that hasn't been fixed yet. With limited resources, there are difficulties that need to be overcome. People want MSN devices that are secure and keep their personal information private, so this paper offers a simple and uncomplicated answer to solve the problem with safe way to protect MSN. The system uses a method called hash-chain based on updating mechanism that uses a key and a signature that is protected by a proxy. A way to make sure data is kept safe while it is being sent and to control who can access it in detail [1].

Our system needs a key that is the same for both encrypting and decrypting and hash operations are used to secure data and are a very suitable choice for small sensors that use less energy. This paper also talks about testing the proposed system in a group of computers to see how it works. Where small gadgets called motes and laptop computers that don't have a lot of resources. It talks about how they perform, getting things done quickly and effectively in real life situations. As far as we know, this is the best information we have. The first system to keep data safe when sending it and control who can access it. Until now, MSNs have not been able to keep your information safe. So, fake health information may be given or handled as authentic because there was no proof that the node was genuine. An adversary means an enemy or opponent, they can add more harmful detectors to the system [4]. Thus, each PAN has a secret master key made up of n secret keys that patient picks and every doctor uses these keys from the certificate authority which has a secret key for unlocking encrypted information. The sensor node took messages and made them secret so no one else could read them. When a doctor sends a prescription to a pharmacy, the pharmacy fills the prescription and provides the medication to the patient. If someone asks for a specific PAN, they can create something. The master key is like a special key for the PAN. To keep IBELite safe and protected, we can't let too many people ask questions. We showed how two parties can check each other's identities and control who can get in.

Many people have written about WSNs, but this text is specifically about ones that are not designed for a specific purpose. Mobile networks that don't need any fixed infrastructure, like cell towers, are called MANETS. These methods cannot be used directly in MSNs because. The special and difficult needs for running and protecting something. A new way to keep access control private by using ring signature technique. In previous studies, a system was developed to manage public keys that is complete and does not require any external resources. A plan has been made for wireless networks that can connect without infrastructure. A little device called a controller is reacting to a target PAN user's request or instruction [2,3].

4. The proposed system

We created a safe and easy-moving system that can be used for wireless medical sensors. It works through networks for patients that have some sensors and a controller. These special devices gather information about the body and health of an individual. Information that includes things like your body temperature, blood pressure, heart rate, and blood sugar levels is called Protected Health Information or PHI. Which are by sensors to the controller. We use techniques called Hash-chain to keep medical data safe. Every time we send data from the sensor to the medical server, we update the key that helps keep it secure. When you sign up, you get a key from the medical server. When someone uses the “proxy key,” they can get into the system and look at a patient's medical information on the medical server. We have a way to code and decode messages using AES algorithm (Fig. 1). The data

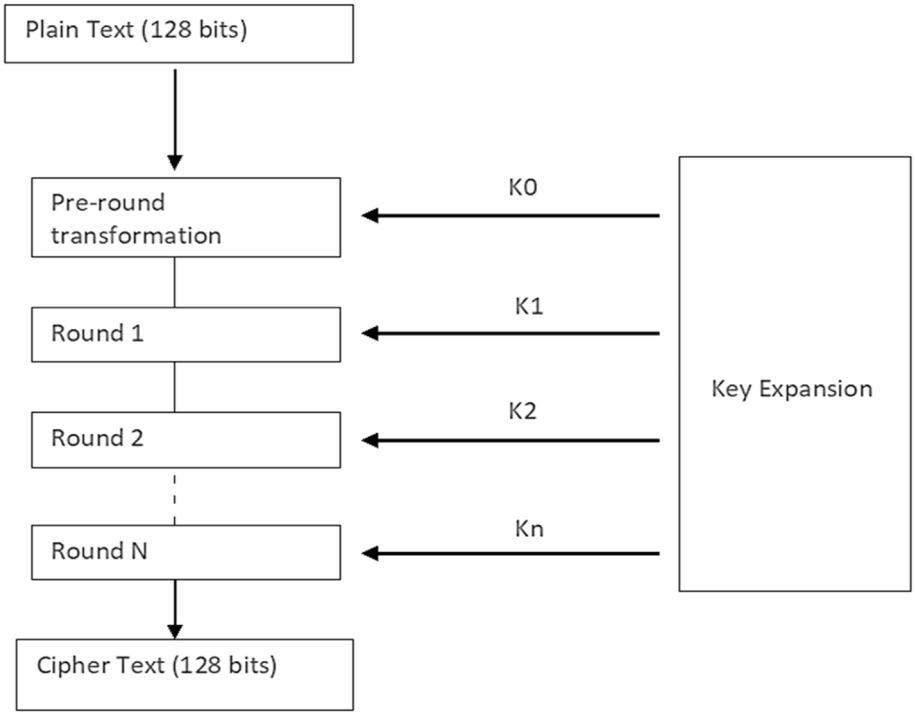

Fig. 1. AES algorithm flowchart.

going from the sensor to the network is kept safe by using this AES algorithm. Also, Doctors get information which has already put into a AES algorithm so no one else can read it [6,7].

4.1. AI for enhancing encryption performance

Encryption Speed Optimization: AI can be used to optimize the performance of the AES algorithm on different platforms [8]. AI models can analyze and adapt the encryption process to maximize speed without compromising security [9–11].

4.2. Positive outcomes

This system doesn't need a lot of computer power or storage space to work with a biosensor [12]. It uses easy ways to keep information safe, like secret codes. We used hashing which is a way to securely store and retrieve data so the system does not have any waiting time. A signature key is used to confirm someone's identity then the user has control over small details [13–15].

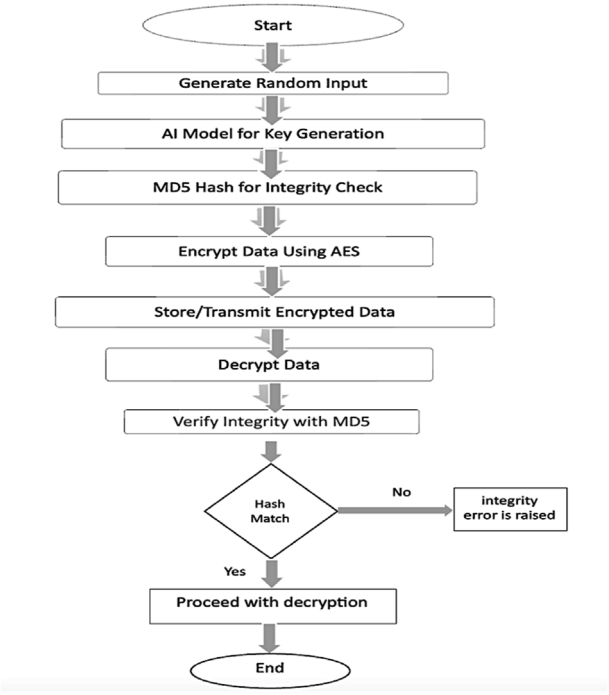

Fig. 2. Proposed system flowchart.

5. Implementation and discussion

When incorporating AI and MD5 (Fig. 2) augmentation of AES (Advanced Encryption Standard) algorithm incorporates AI into some components of AES, like key management, security assessment, or performance. Some parts of the enhancement process use MD5, for instance for integrity checks, or as part of a non-critical pre-processing [7]. Here's how you might go about it:

- AI for Secure Key Generation: Next, instead of the current methods for AES key generation, various AI algorithms (neural networks, genetic algorithms, reinforcement learning) could be used to create random virtually impossible to guess keys. This can prove to enhance the complexity and additional level of security.
- Using MD5 for Key Hashing: With MD5 to convert the key or the password used to encrypt data using AES. AI may enhance the key space such that even when weak passwords are being used; enhanced encrypted keys will be developed.

Proposed System Architecture:

1. Key Generation: generate a high-entropy key for AES encryption.
2. Hashing: Hash the key or sensitive data with MD5
3. Encryption: Encrypt the data using AES, with AI-based optimizations for the encryption process.
4. Verification: Use the MD5 hash of the original plaintext to verify data integrity after decryption.

Flowchart Description:

1. Generate Random Input: generating random input values to feed into the AI model.
2. AI Model for Key Generation: the model processes the random input and generates a 256-bit AES key.
3. MD5 Hash for Integrity Check: The system computes the MD5 hash of the generated AES key to check its integrity.
   - Store MD5 Hash for later verification.
4. Encrypt Data Using AES: encrypting the plaintext using the AES key.
5. Store/Transmit Encrypted Data: The encrypted data is stored or transmitted securely.
6. Decrypt Data: Upon receiving or retrieving the encrypted data, the system uses the same AES key to decrypt it.
7. Verify Integrity with MD5: computing the MD5 hash of the AES key used for decryption and verifying it against the stored hash.
   - Hash Match?
     - Yes: Proceed with decryption and return the original data.

```python
import numpy as np
import tensorflow as tf

# Create a simple neural network to generate a key
def create_key_generation_model():
    model = tf.keras.Sequential([
        tf.keras.layers.Dense(128, input_shape=(16,), activation='relu'),
        tf.keras.layers.Dense(256, activation='sigmoid')  # Output layer with 256
    ])
    model.compile(optimizer='adam', loss='mse')
    return model

# Generate a random input to feed into the AI model
def generate_random_input():
    return np.random.rand(1, 16)

# Use the AI model to generate a key
def generate_aes_key(model):
    random_input = generate_random_input()
    key = model.predict(random_input)
    key = (key * 255).astype(np.uint8)  # Convert to 256-bit integer values
    return key.tobytes()[:32]  # Return 32 bytes (256 bits) as the AES key

# Create and train the model (for simplicity, no training here)
model = create_key_generation_model()

# Generate the AES key using the AI model
aes_key = generate_aes_key(model)
print(f"Generated AES Key: {aes_key.hex()}")
```

- No: An integrity error is raised, meaning the key or data may have been tampered with.

The proposed system deals with low security input and then acquires high security key for encrypting patient data. Therefore, attacking the system for breaking encrypted data will cost more time and experience and my result rubbish information after decryption process.

AI Model for Key Generation Coded in Python:

6. Conclusion

We suggested a secure and light system for wireless medical devices. To keep medical information safe, AI way in send this information in high security method which makes sure that only the right people can see it. The hash-chain based key mechanism and the proxy key signature technique are used MD5 with AI worked together to add complexity lyres to the sent information. Thus, make sure that private healthcare information is sent and received safely using wireless devices, and control who can access it.

Funding

Self-funding.

References

[1] Li M, Lou W, Ren K. Data security and privacy in wireless body area networks. IEEE Wireless Commun 2010;17(1):51−8.
[2] Al-Janabi S, Al-Shourbaji I, Shojafar M, Shamshirband S. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egypt Inform J 2017;18(2):113−22.
[3] Rashmi Kumari. A study on wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. Int J Adv Res Comput Commun Eng 2017;6(1): 403−5.
[4] Javadi SS, Razzaque MA. Security and privacy in wireless body area networks for health care applications. Wireless Netw Sec: Iss Challenge Res Trends 2013:165−87.
[5] Rghioui A, L'aarje A, Elouaai F, Bouhorma M. Protecting e-healthcare data privacy for internet of things based wireless body area network. Res J Appl Sci Eng Technol 2015;9(10): 876−85.
[6] Abdullah AM. Advanced encryption standard (AES) algorithm to encrypt and decrypt data. Cryptograph Netw Sec 2017;16(1):11.
[7] Zeghid M, Machhout M, Khriji L, Baganne A, Tourki R. A modified AES based algorithm for image encryption. Int J Comp Inform Eng 2007;1(3):745−50.
[8] Palm G. The PAN system and the WINA project. InEuropäischer Informatik Kongreß Architektur von Rechensystemen Euro-ARCH'93: München, 18.−19. Springer Berlin Heidelberg; 1993. p. 142−56. Oktober 1993.
[9] Lea P. Internet of Things for Architects: architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security. Packt Publishing Ltd; 2018.
[10] Al-Qatatsheh A, Morsi Y, Zavabeti A, Zolfagharian A, Salim N, Z. Kouzani A, et al. Blood pressure sensors: materials, fabrication methods, performance evaluations and future perspectives. Sensors 2020;20(16):4484.
[11] Umoga UJ, Sodiya EO, Ugwuanyi ED, Jacks BS, Lottu OA, Daraojimba OD, et al. Exploring the potential of AI-driven optimization in enhancing network performance and efficiency. Magna Scientia Adv Res Rev 2023;10(1):368−78.
[12] Al-Neaimi AM, Hassan RF. New approach for modifying blowfish algorithm by using multiple keys. IJCSNS 2011; 11(3):21.
[13] Koehler S, Dhameliya N, Patel B, Anumandla SK. AI-enhanced cryptocurrency trading algorithm for optimal investment strategies. Asian Account Audit Adv 2018;9(1): 101−14.
[14] Patel K, Beeram D, Ramamurthy P, Garg P, Kumar S. Ai-enhanced design: revolutionizing methodologies and workflows. Int J Artif Intel Res Develop (IJAIRD) 2023;2(1):135−57.
[15] Chinnam Y, Sambana B. Artificial intelligence enhanced security problems in real-time scenario using blowfish algorithm. arXiv preprint arXiv:2023.09286 2023;16(1):50−62.