PRIVATE AND SECURED MEDICAL DATA TRANSMISSION AND ANALYSIS FOR WIRELESS SENSING HEALTH CARE SYSTEM

Abstract

This report presents a system for secure medical data transmission and real-time analysis within wireless sensing healthcare frameworks. Leveraging IoT, body-area networks (BANs), and secure data protocols, the system facilitates remote monitoring of vital health parameters, ensuring privacy and efficiency. The proposed solution integrates Python 3.5 for data handling and visualization, with real-time web server updates. Key advancements include low-power wearable sensors, encrypted data transmission, and anomaly detection for improved healthcare outcomes.

RESEARCH OBJECTIVE

The primary objective of this research is to enhance the security of health data transmission in IoMT frameworks by proposing and evaluating a novel key generation scheme.

1. Introduction

The rise of wireless healthcare technologies marks a transformative phase in modern medicine. With the integration of IoT and wearable sensors, healthcare systems can provide continuous monitoring of patients' vital parameters, including pulse rate, blood pressure, and temperature. However, safeguarding patient data from unauthorized access is critical.

India's healthcare system exhibits disparities between urban and rural areas. This project addresses these challenges by deploying IoT-enabled medical systems to bridge the gap in healthcare services. The incorporation of wireless sensor networks (WSNs) and privacy-preserving protocols enhances the reliability and accessibility of medical care.

s it more inescapable. Utilizing IOT we can ready to interface gadgets and cooperate with sensor,. Due to this reason IOT was utilized as a part of medicinal services framework. In our task we utilize IOT and distinctive wearable sensors which can ready to get the data from our human organs and body and the processor utilized will compute the data. We will utilize sensors in wellbeing observing framework, which will make the checking framework all the more intense anyplace, whenever. With this enhances the period of individuals which enhances the personal satisfaction.

Web server data can be observed by the doctor's facility staff like specialists and can ready to prudent strides at the crisis level.

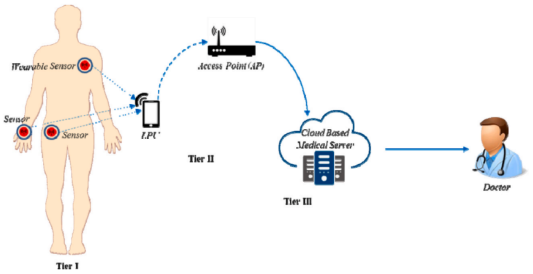


Fig. 1. Architecture of IoMT-based healthcare system.

2. Literature Review

2.1 Previous Systems

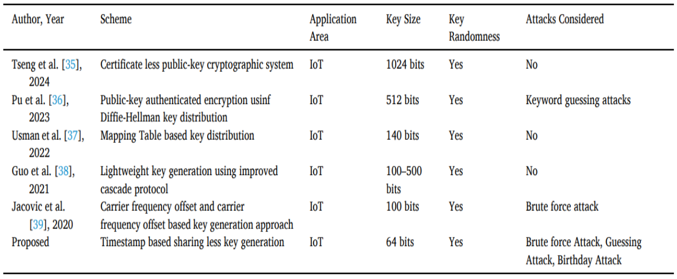
Conventional healthcare monitoring systems relied on Bluetooth-based devices for short-range communication. Although effective for single-patient monitoring, these systems faced limitations like high power consumption, low data security, and restricted range.

2.2 Advancements in IoT and WBANs

The convergence of IoT, WBANs, and cloud computing has introduced a paradigm shift in e-healthcare. Modern systems allow real-time data sharing across secure web servers, enabling medical practitioners to access patient data remotely. This transition has improved disease diagnosis and management.

4. Related works

Table 1
Recent key generation techniques for IoT.



Author, Year	Scheme	Application Area	Key Size	Key Randomness	Attacks Considered
Tseng et al. [35], 2024	Certificate less public-key cryptographic system	IoT	1024 bits	Yes	No
Pu et al. [36], 2023	Public-key authenticated encryption usinf Diffie-Hellman key distribution	IoT	512 bits	Yes	Keyword guessing attacks
Usman et al. [37], 2022	Mapping Table based key distribution	IoT	140 bits	Yes	No
Guo et al. [38], 2021	Lightweight key generation using improved cascade protocol	IoT	100–500 bits	Yes	No
Jacovic et al. [39], 2020	Carrier frequency offset and carrier frequency offset based key generation approach	IoT	100 bits	Yes	Brute force attack
Proposed	Timestamp based sharing less key generation	IoT	64 bits	Yes	Brute force Attack, Guessing Attack, Birthday Attack

Using the secret key the adversary can decrypt the data and see or alter it. As a consequence, security requirement of secret key is also a big concern. To overcome and reduce the security attacks, exploration is needed so that secret key need not be shared with receiver for decryption. This motivated us to design a Simple Novel Key Generation Scheme (SKG) where without sharing secret key encryption and decryption is possible, only secret information required to regenerate secret key at receiver end is shared.

5. Proposed methodologies

In IoT enabled healthcare applications sensors and other devices are energy constraint and computational ability is also less [46]. Thus, to design a framework with less complexity and faster data transmission speed ensuring confidentiality is a challenging task. To overcome this challenge, a novel secret key generation scheme and a secure data transmission framework is proposed

5.1. Secret key generation (SKG) scheme

In typical symmetric key cryptography, encryption key must be shared with the receiver to decrypt data, which is a big challenge and vulnerable to various security threats. But in our scheme key sharing is not required, which reduces the number of security attacks. Date and time from the devices used in patient and doctor end is the input to form a 64-bit secret key. Data and time elements such as mm - minute, HH - hour, DD-date, MM-month, YYYY- Year have been used. System date and time are fetched at first in mmHHDDMMYYYY format. The respective value of this format is then converted to its binary form. But the values are less than 64 bits, so to overcome this, first 32 bits from the binary value is selected and the values are then inversed. Now 2x32 values are there including original and inversed values. Both the values are then concatenated to form a 64-bit binary value. This binary could have been used as a secret key, but it is found that binary numbers can be easily found by Brute Force. So, the 64-bit binary value is converted to Hexa decimal value, which is more complex to be found by Brute force method. This 64 bit or 16 character Hex has been used as secret key in our proposed secure data transmission framework.

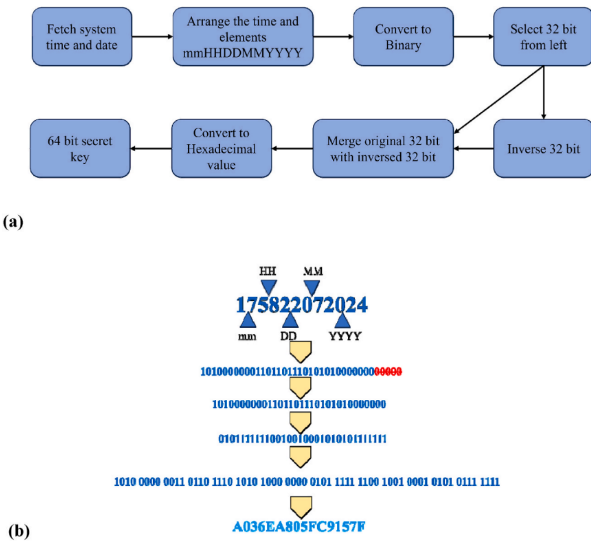


Fig. 2. (a) Block diagram of key generation scheme. Fig. 2 (b) Example of a key generation.

application in resource constraint PDA devices. Attack model and resilience analysis has been discussed in later sections. To measure the strength of key, complexity in number of bits is calculated which is often called Entropy [47]. Eq. (1) is the formula to calculate.

Entropy = log2NL

Here N is the cardinality and L is the length of the key. Cardinality refers to the contents of key element, Hex uses combination 0–9 (Ten) and A-F (Six) characters. So, the value of cardinality is 16 and 64 bit refers to 16 Hex characters, so the Length is 16. The entropy calculation using equation (1) reveals that the Hex key has an entropy of 64 bits, whereas the decimal key has an entropy of 16 bits. Consequently, the Hex key is stronger and more suitable.

5.2. Secure data transmission framework

Confidentiality of health data is one of critical security requirement in IoMT. This requirement can be satisfied using traditional cryptographic algorithms. Symmetric cryptographic algorithms are considered to be faster than asymmetric, because it is less complex in nature This paper presents a secure framework for transmitting health vitals from a sensor device to a doctor device using Cloud technology. The framework employs DES encryption, combined with a custom key generation scheme, to protect sensitive health data. DES is a popular symmetric cryptographic algorithm widely chosen by various researchers in IoMT . Proposed Secure data transmission framework uses two handheld devices with limited resources and Wi-Fi internet connectivity, one for the patient and another for the doctor. System time and date of both the device need to be synchronized and key generation scheme has to be agreed. The body vitals are measured by the wearable sensor device and aggregation is done by the patient device. Then secret key is generated using our key generation scheme, using that key health vitals are encrypted and forwarded to the Cloud database using internet. At the doctor end, the encrypted data is retrieved from the cloud database and the same key generation scheme is used to corresponding the same key. Using the key, the health data is decrypted and doctor can see the information in a meaningful format.

Algorithm 1: Secure data transmission using key generation scheme

```
BEGIN:
Procedure: key generation, encryption and transmission of
$fori = 1$ to n do
$v[i] =$ collect body vitals from dataset
```

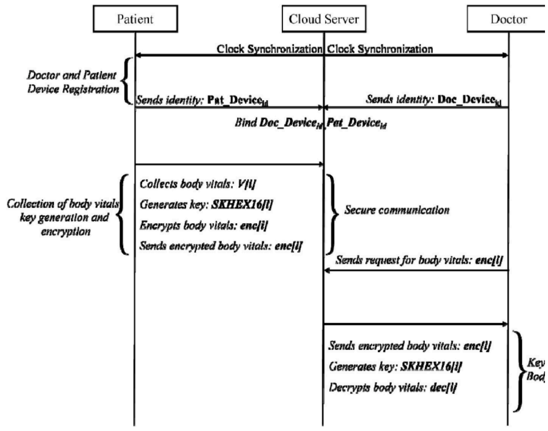

Patient
Cloud Server
Doctor
Clock Synchronization
Clock Synchronization
Doctor and Patient Device Registration
Sends identity: Pat_Device$_{Id}$
Sends identity: Doc_Device$_{Id}$
Bind Doc_Device$_{Id}$ Pat_Device$_{Id}$
Collection of body vitals key generation and encryption
Collects body vitals: V[i]
Generates key: SKHEX16[i]
Encrypts body vitals: enc[i]
Sends encrypted body vitals: enc[i]
Secure communication
Sends request for body vitals: enc[i]
Sends encrypted body vitals: enc[i]
Generates key: SKHEX16[i]
Decrypts body vitals: dec[i]
Key
Bod

Fig. 3. Proposed Secure health data transmission framework for IoMT.

7. Implementation and experimental setup

Proposed secure data transmission framework has been implemented using PHP and MySQL, user interface has been designed using HTML and CSS.Wearable sensors such as SPO2, Body Temperature and ECGhas been employed for the collection body vitals.Body temperature sensors is positioned on the left arm, a Spo2 sensor is positioned on the right index finger, and ECG probes are positioned over the chest and abdomenshown in Fig. 4 and sensor values has been shown in Fig. 5. Mysignals [58] HW Shield and Arduino has been used as the microcontroller device which is connected to the internet using ESP8266 wireless module.The PHP-based doctor and patient portal allows both parties to log in using their login information to examine the health vitals.AWS cloud-based MySQL database has been utilized for storage of encrypted health data as shown in Table 4. Proposed key generation scheme is implemented in both patient and doctor device. A microcontroller is considered as a patient device, while a laptop serves as a doctor device in this scenario. Patient device is responsible for secret key generation, encryption using DES and transmission to the cloud storage. Doctor devices can retrieve the encrypted health record and decrypt it. Initially, an interval of 1 ms is set to collect sensor data and transmit it securely to the doctor.

Table 3
Brute force attack simulation result for various sequence.

Key Size(bit)	Elements	Threshold time	Time to discover
28	YYYYMMDD	60min	4 s
32	YYYYMMDD	60min	45 s
48	YYYYMMDD	60min	58 min
64	mmHHDDMMYYYY	60min	Not found

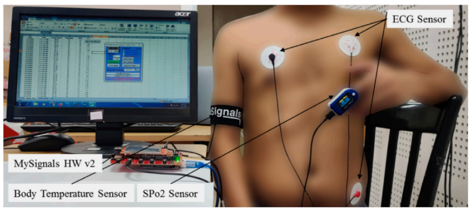
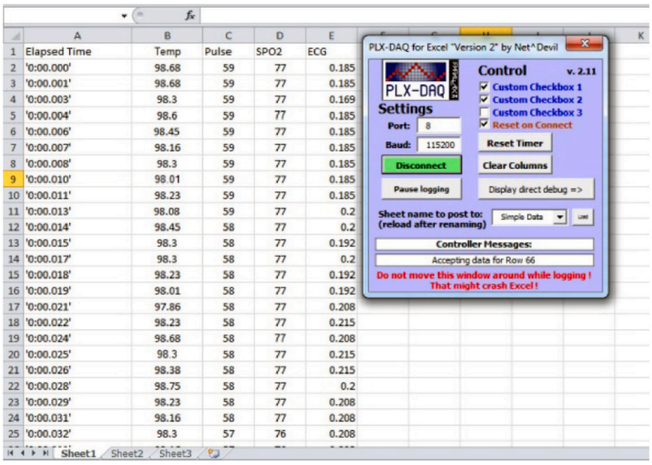


Fig. 4. IoMT based Experimental setup for health data collection.



	A	B	C	D	E
1	Elapsed Time	Temp	Pulse	SPO2	ECG
2	'0:00.000'	98.68	59	77	0.185
3	'0:00.001'	98.68	59	77	0.185
4	'0:00.003'	98.3	59	77	0.169
5	'0:00.004'	98.6	59	77	0.185
6	'0:00.006'	98.45	59	77	0.185
7	'0:00.007'	98.16	59	77	0.185
8	'0:00.008'	98.3	59	77	0.185
9	'0:00.010'	98.01	59	77	0.185
10	'0:00.011'	98.23	59	77	0.185
11	'0:00.013'	98.08	59	77	0.2
12	'0:00.014'	98.45	58	77	0.2
13	'0:00.015'	98.3	58	77	0.192
14	'0:00.017'	98.3	58	77	0.2
15	'0:00.018'	98.23	58	77	0.192
16	'0:00.019'	98.01	58	77	0.192
17	'0:00.021'	97.86	58	77	0.208
18	'0:00.022'	98.23	58	77	0.215
19	'0:00.024'	98.68	58	77	0.208
20	'0:00.025'	98.3	58	77	0.215
21	'0:00.026'	98.38	58	77	0.215
22	'0:00.028'	98.75	58	77	0.2
23	'0:00.029'	98.23	58	77	0.208
24	'0:00.031'	98.16	58	77	0.208
25	'0:00.032'	98.3	57	76	0.208

PLX-DAQ for Excel "Version 2" by Net^Devil

Control v. 2.11

☑ Custom Checkbox 1
☑ Custom Checkbox 2
☐ Custom Checkbox 3
☑ Reset on Connect

Settings
Port: 8
Baud: 115200

Sheet name to post to: (reload after renaming) Simple Data

Controller Messages:
Accepting data for Row 66

Do not move this window around while logging ! That might crash Excel !

Fig. 5. Health data samples collected using body sensors.

8. Results and analysis

For performance analysis three experiments have been conducted for three block cipher modes of DES such as ECB,CBC and CTR. Each experiment includes secure health data transmission for 60 min, thus a total 180 min of data transmission takes place from patient device to doctor device. In first phase DES has been configured in ECB mode and the time required for various operations as per al gorithm 1 has been recorded. Similar approach has been followed for DES with CBC and CTR mode respectively. Fig. 7 (a) (b) and (c) show time required by 10 transmissions for DES-ECB, DES-CBC and DES-CTR modes respectively.

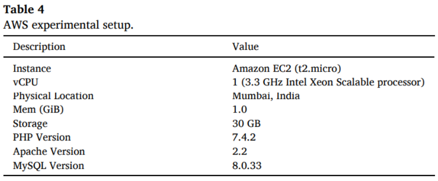
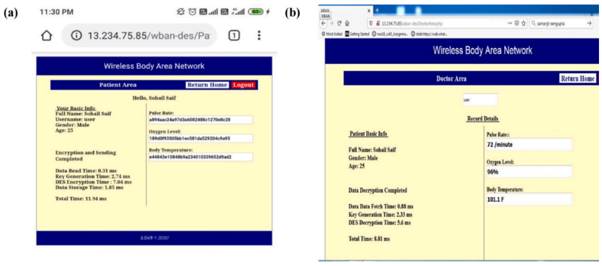


Table 4
AWS experimental setup.

Description	Value
Instance	Amazon EC2 (t2.micro)
vCPU	1 (3.3 GHz Intel Xeon Scalable processor)
Physical Location	Mumbai, India
Mem (GiB)	1.0
Storage	30 GB
PHP Version	7.4.2
Apache Version	2.2
MySQL Version	8.0.33



Hello, Sohail Saif

Your Basic Info
Full Name: Sohail Saif
Username: user
Gender: Male
Age: 25

Encryption and Sending Completed

Data Read Time: 0.31 ms
Key Generation Time: 2.74 ms
DES Encryption Time : 7.04 ms
Data Storage Time: 1.85 ms

Total Time: 11.94 ms

Pulse Rate: a894aac24a97d3a6082488c1270e8c28
Oxygen Level: 189d0f93505bb1ec581da529204c9a95
Body Temperature: e44843e10848b9a234010339652d9ad2

user

Record Details

Patient Basic Info

Full Name: Sohail Saif
Gender: Male
Age: 25

Data Decryption Completed

Data Data Fetch Time: 0.88 ms
Key Generation Time: 2.33 ms
DES Decryption Time: 5.6 ms

Total Time: 8.81 ms

Pulse Rate:: 72 /minute
Oxygen Level: 96%
Body Temperature: 101.1 F

Fig. 6. User interface of patient and doctor device during data transmission.

9. Conclusion and future research

directions This paper proposes a novel key generation scheme and a secure data transmission framework specifically designed for IoT-based health monitoring applications. Our approach generates secret keys at the receiver's end, eliminating the need for key sharing. System date and time are used for key generation independently on patients' and doctors' devices. Security attacks including Guessing or Mask attacks, Brute Force attacks, and Birthday attacks were simulated to assess resilience. Proposed scheme showed 91 % and 100 % safety against Guessing or Mask attacks and Brute Force attacks, respectively, and demonstrated robustness against Birthday attacks. A secure data transmission framework was developed by applying this scheme to DES. The performance of three cipher block modes (ECB, CBC, and CTR) was analyzed. Health data collected via body sensors was transmitted using this framework.

References

[1] B.L.Y. Agbley, et al., Federated Fusion of Magnified Histopathological Images for Breast Tumor Classification in the Internet of Medical Things, in: IEEE Journal of Biomedical and Health Informatics 28, Institute of Electrical and Electronics Engineers (IEEE, Jun. 2024, pp. 3389–3400, https://doi.org/10.1109/ jbhi.2023.3256974.

[2] A.U. Haq, J.P. Li, I. Khan, B.L.Y. Agbley, S. Ahmad, M.I. Uddin, I. Alam, DEBCM: deep learning-based enhanced breast invasive ductal carcinoma classification model in IoMT healthcare systems, IEEE Journal of Biomedical and Health Informatics 28 (3) (2022) 1207–1217. [

3] O. Samuel, A.B. Omojo, A.M. Onuja, Y. Sunday, P. Tiwari, D. Gupta, Shamshirband, S. IoMT, A COVID-19 healthcare system driven by federated learning and blockchain, IEEE Journal of Biomedical and Health Informatics (2022).

[4] A.K. Das, B. Bera, D. Giri, Ai and blockchain-based cloud-assisted secure vaccine distribution and tracking in iomt-enabled covid-19 environment, IEEE Internet of Things Magazine 4 (2) (2021) 26–32.

[5] M.A. Khelili, S. Slatnia, O. Kazar, S. Harous, IoMT-fog-cloud based architecture for Covid-19 detection, Biomed. Signal Process Control 76 (2022) 103715.

[6] F. Alsubaei, A. Abuhussein, V. Shandilya, S. Shiva, IoMT-SAF: internet of medical things security assessment framework, Internet of Things 8 (2019) 100123.

[7] P. Bhadra, S. Chakraborty, S. Saha, Cognitive IoT meets robotic process automation: the unique convergence revolutionizing digital transformation in the industry 4.0 era, in: Confluence of Artificial Intelligence and Robotic Process Automation, Springer Nature Singapore, Singapore, 2023, pp. 355–388.

[8] S. Wang, Q. Sun, Y. Shen, X. Li, Applications of robotic process automation in smart governance to empower COVID-19 prevention, Procedia Comput. Sci. 202 (2022) 320–323.

[9] A.J. Bindiya, N. Anitha, S. Indumathi, Robotic Process Automation (RPA): a software bot for healthcare sector, in: 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), IEEE, 2023, January, pp. 685–689.

[10] R. Kumar, R. Tripathi, Towards design and implementation of security and privacy framework for internet of medical things (iomt) by leveraging blockchain and ipfs technology, J. Supercomput. 77 (8) (2021) 7916–7955.

[11] V. Kumar, M.S. Mahmoud, A. Alkhayyat, J. Srinivas, M. Ahmad, A. Kumari, RAPCHI: robust authentication protocol for IoMT-based cloud-healthcare infrastructure, J. Supercomput. (2022) 1–30.