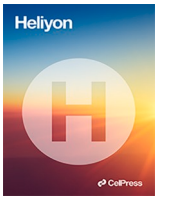
Heliyon 10 (2024) e36269

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon



Research article

A secure data transmission framework for IoT enabled healthcare

Sohail Saif [a], Priya Das [b], Suparna Biswas [c], Shakir Khan [d,e], Mohd Anul Haq [f], Viacheslav Kovtun [g,*]

[a] Department of Computer Applications, Maulana Abul Kalam Azad University of Technology, Haringhata, 741249, India
[b] Department of Computer Science, Chakdaha College, Chakdaha, 741222, India
[c] Department of Computer Science & Engineering, Maulana Abul Kalam Azad University of Technology, Haringhata, 741249, India
[d] College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, 11432, Saudi Arabia
[e] University Centre for Research and Development, Chandigarh University, Mohali, 140413, India
[f] Department of Computer Science, College of Computer and Information Sciences, Majmaah University, Al-Majmaah, 11952, Saudi Arabia
[g] Computer Control Systems Department, Vinnytsia National Technical University, Vinnytsia, Ukraine

ARTICLE INFO

Keywords:
IoT
Encryption
Security
Healthcare
IoMT

ABSTRACT

The Internet of Medical Things (IoMT) has transformed healthcare by connecting medical devices, sensors, and patients, significantly improving patient care. However, the sensitive data exchanged through IoMT is vulnerable to security attacks, raising serious privacy concerns. Traditional key sharing mechanisms are susceptible to compromise, posing risks to data integrity. This paper proposes a Timestamp-based Secret Key Generation (T-SKG) scheme for resource-constrained devices, generating a secret key at the patient's device and regenerating it at the doctor's device, thus eliminating direct key sharing and minimizing key compromise risks. Simulation results using MATLAB and Java demonstrate the T-SKG scheme's resilience against guessing, birthday, and brute force attacks. Specifically, there is only a 9 % chance of key compromise in a guessing attack if the attacker knows the key sequence pattern, while the scheme remains secure against brute force and birthday attacks within a specified timeframe. The T-SKG scheme is integrated into a healthcare framework to securely transmit health vitals collected using the MySignals sensor kit. For confidentiality, the Data Encryption Standard (DES) with various Cipher Block modes (ECB, CBC, CTR) is employed.

1. Introduction

The rapid advancement of technology has been profoundly transforming various industries, and the healthcare sector is no exception. Among the groundbreaking innovations emerging in recent years, the Internet of Medical Things (IoMT) has emerged as a revolutionary concept that holds immense potential to revolutionize healthcare delivery and patient outcomes [1]. IoMT represents the integration of medical devices, applications, and systems with Internet of Things (IoT) technology, creating a network of interconnected devices and data in the healthcare ecosystem [2]. IoMT enables medical devices, wearables, sensors, and other healthcare-related equipment to collect and exchange valuable data in real-time. This interconnectedness allows healthcare professionals to monitor patients remotely, gain insights into their health conditions, and make informed decisions for personalized

* Corresponding author.
E-mail addresses: sohailsaif7@gmail.com (S. Saif), 28priyadas@gmail.com (P. Das), mailtobiswas.suparna@gmail.com (S. Biswas), sgkhan@imamu.edu.sa (S. Khan), m.anul@mu.edu.sa (M.A. Haq), kovtun_v_v@vntu.edu.ua (V. Kovtun).

https://doi.org/10.1016/j.heliyon.2024.e36269
Received 7 February 2024; Received in revised form 7 August 2024; Accepted 13 August 2024
Available online 14 August 2024

treatments [3].

Fig. 1 shows the traditional architecture of IoMT, which includes sensor devices, a coordinator device, and a cloud medical server. These sensors are wirelessly connected (short range) to a Local Processing Unit (LPU) which can be a laptop, smartphone, etc. After processing in LPU, the data goes to the Cloud-Based Medical (CBM) server. The medical team and doctors can remotely access this data and diagnose patient conditions. Additionally, patients can actively participate in managing their own health by accessing real-time data and receiving timely feedback and support.

The vast applications of IoMT span across various healthcare domains, including remote patient monitoring, chronic disease management, telemedicine, hospital asset management, medication adherence, and healthcare supply chain optimization [4–6]. By facilitating seamless data transmission, IoMT has the potential to improve medical accuracy, enhance patient engagement, reduce healthcare costs, and ultimately, save lives.

Nevertheless, the incorporation of technology into the delicate realm of healthcare necessitates careful consideration of challenges such as data privacy, security, interoperability, and regulatory compliance [7–9]. Striking the right balance between harnessing the power of IoMT and safeguarding patient privacy and security is crucial to ensuring its successful implementation [10–12]. Healthcare data contains highly sensitive and personal information, including patient records, medical histories, and diagnostic data.

The interconnected nature of IoMT devices makes the entire ecosystem vulnerable to cyber threats, which could lead to devastating consequences, including unauthorized access to patient data, tampering with medical devices, Denial-of-Service (DoS) Attacks, Man-in-the-Middle (MITM) Attacks due to the lack of standardized security protocols and guidelines across the IoMT ecosystem [13–15]. All of the applications of IoMT use sensors and actuators to collect various data and perform several tasks, including health data collection.

Since patient health information is transmitted through this Body Sensor Network and stored in medical servers, these data are vulnerable to security threats. In a real-time scenario, patients' information should be available all the time on the server so that in case of any critical condition, the medical team can take action as soon as possible [16,17]. As data are always available, attackers may target the communication medium or sometimes the electronic object to steal the information of patients.

Security attacks in the healthcare system could be targeted at any of three levels: At the sensing layer-sensor devices could be compromised, communication layer-network channels, processing, or storage layer-cloud medical server can be compromised. This work focuses on securing health information in transit, i.e., at the communication layer as well as in cloud-based storage, by applying cryptographic approaches. This urgency for robust security measures drives the development of innovative secret key generation techniques [18–20].

2. 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.

3. Contributions

- Identification of various security threats in IoMT-based data transmission framework, motivating the proposal of a secure data transmission framework incorporating a novel key generation scheme.
- Utilization of cipher block modes such as Electronic Code Book (ECB), Cipher block chaining (CBC), and Counter (CTR) with DES for performance comparison and analysis.
- Simulation of three security attacks on secret keys such as Guessing attack, birthday, and Brute Force attack using Matlab and Java to assess the resilience of our key generation scheme.

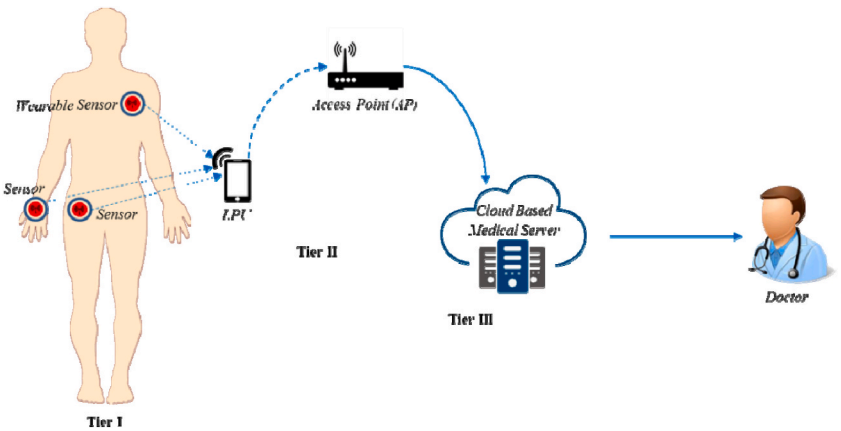


Fig. 1. Architecture of IoMT-based healthcare system.

- Utilization of IoMT-based framework for the collection of health vitals such as SPO2, Body Temperature, and ECG from the human body.
- Consideration of evaluation parameters such as transmission time and packet delivery rate, with detailed simulation results discussed.

The remaining sections of the paper are structured as follows: Section 2 presents recent related research. Our proposed methodologies are outlined in Section 3. Section 4 introduces the attack model, while Sections 5 and 6 detail the implementation process and experimental results. Ultimately, Section 7 draws the paper to a conclusion.

4. Related works

Security has become one of the biggest problems in any IoMT-based healthcare system since patient health records is so sensitive. Key management is one technique for maintaining this system's security intact.The fundamental goal of key management is to create, distribute, and to preserve keys until they are destroyed. IoT devices cannot use conventional key distribution systems due to resource constraints. This section reports recent research works on lightweight key management techniques and secure communication framework for IoMT. SKYGlow is a secret key generation technique for resource constrained IoT device [21]. This scheme utilizes Discrete Cosine Transform (DCT) on communication channel observations of sent messages to maximize correlation between the generated secret key bits. Soni et al. [22] presented a symmetric secret key generation for IoT networks based on the wireless channel parameter such received signal strength (RSS). With the help of correlated colored noise components author proposed a low complexity filtering approach that can enhanced the performance of the RSS signal-based key generation approach. Chen et al. [23] proposed an efficient secret key generation approach for the one-time pad encryption algorithm, which was based on AES. The proposed scheme generated secret keys for secure communication between IoT devices and Edge server devices. Simulations were conducted to verify the feasibility and correctness of the proposed scheme. Tang et al. [24] proposed a Group key generation technique for multiple IoT devices. The proposed scheme reduced the reliance on channel probing techniques, making the scheme more efficient and cost-effective.Usman et al. [25] presented another energy-efficient key distribution procedure at the physical layer. The proposed scheme combined multiple characteristics of the communication channel, resulting in a significant improvement in key generation rate.Coelho et al. [26] introduced LORENA, a low-memory symmetric-key generation technique for Internet of Health Things (IoHT). LORENA utilized ECG signals to generate a 128-bit shared secret key between IoHT sensor nodes.Das and Namusudra [27] presented a hybrid encryption technique for securing IoT-enabled healthcare data. The technique combined well-known encryption algorithms such as ECC, AES, and Serpent. These algorithms were fused together to encrypt IoT health data, with the required public-private key pairs generated during the registration phase.Kumar et al. [28] described the Rooted Elliptic Curve Cryptography with Vigenère cipher (RECC-VC) security scheme. This proposed scheme enhanced IoMT security through the implementation of an exponential K-anonymity algorithm. RECC-VC facilitated the secure transmission of human health data from IoMT network to cloud servers.Sultana et al. [29] introduced a homomorphic encryption approach that relies on transformed ASCII values assigned to individual characters in plaintext. In their proposed system, the generated secret key utilized a tetrahedral-based and a Pentatope-based configuration. Iqbal et al. [30] introduced a secure and efficient key management approach for Wireless Body Sensor Networks (WBSNs). The proposed scheme employed CP-ABE for health data encryption and consortium blockchain for authentication and key management. Fixed-size session keys were generated through attribute-based rules and AND/OR logic. Kumar et al. [31] presented a Constrained Application Protocol (CoAP)-based secure data transmission framework for an IoT-based smart building. Datagram Transport Layer Security (DTLS) was used for message encryption, while SHA-256 was employed for key generation and sharing. The proposed framework was simulated using the COOJA simulator for 90 min. Experimental results demonstrate that energy consumption is lowered by approximately 30.86 %. Several other authors suggested the use of blockchain framework for health data security [32,33].Steganography is another technique which can be used to secure medical images [34].A comparative summary of key generation techniques considered by the authors in recent years has been shown in Table 1.

Upon reviewing numerous research papers and surveys, certain areas for improvement became apparent. In much of the related

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

literature, secret keys were transmitted from sender to receiver in plaintext, leaving them vulnerable to channel attacks. Some authors resorted to encryption or hash functions to secure these keys [40–42], resulting in increased computational overhead.In some of the works, the basic security requirements such as privacy, integrity, freshness, authentication, anonymity, secure localization as demanded in real applications are not maintained [43–45]. Also, it is observed that researchers have considered the security parameters in their proposal, but only few authors considered the security issue in secret key sharing. If secret key is not shared in a secure way and if the adversary gets the key, then they can easily decrypt the data. Therefore, the whole security scheme will be jeopardized. 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 Hexadecimal 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. For better representation and understanding key generation process with example are shown in Fig. 2 (a) and 2 (b). This scheme is less complex as well as secure from security attacks which make it suitable for

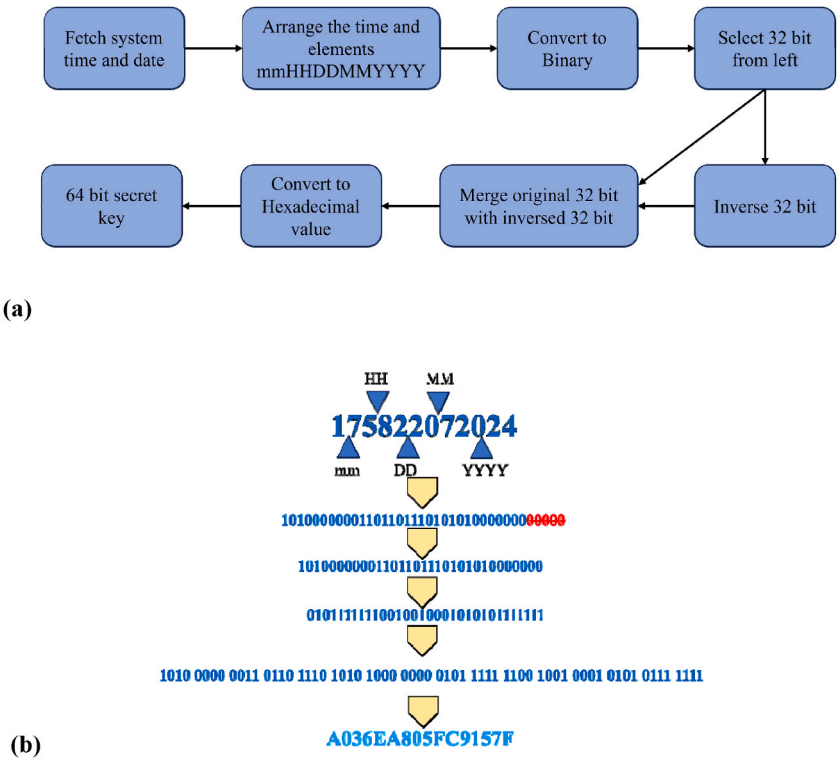


Fig. 2. (a) Block diagram of key generation scheme. Fig. 2 (b) Example of a key generation.

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.

$$Entropy = log_2 N^L \tag{1}$$

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 [48–50]. 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. This framework secures the health data in transit as well as in storage. Entire process has been shown in Algorithm 1 and the proposed secure framework has been reflected in Fig. 3.

Algorithm 1: Secure data transmission using key generation scheme

1:	BEGIN:
2:	Procedure: key generation, encryption and transmission of health data (patient's device)
3:	***for*** i = 1 to n do
4:	v[i] = collect body vitals from dataset

(*continued on next page*)

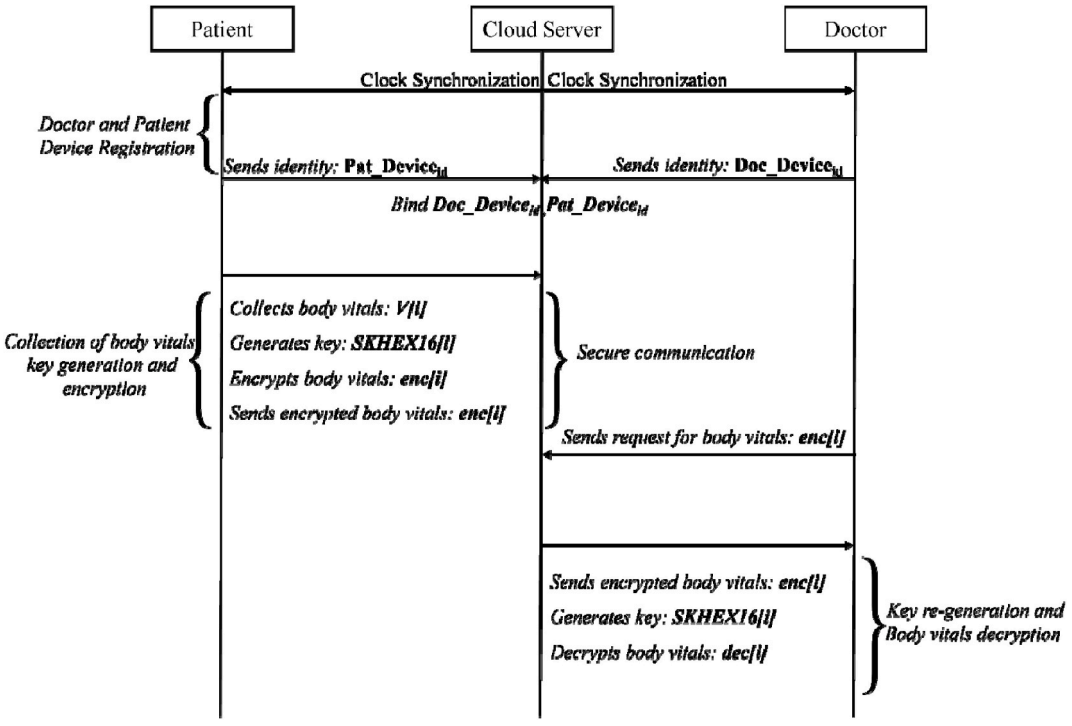


Fig. 3. Proposed Secure health data transmission framework for IoMT.

(*continued*)

Algorithm 1: Secure data transmission using key generation scheme	
5:	DTIM [i] = [mm||HH||DD||MM||YYYY]
6:	BIN[i] = converted in binary
7:	BIN32[i] = select 32 bit from left
8:	BIN32′[i] = inverse
9:	bin64[i] = [BIN32[i]|| BIN32′[i]]
10:	SKHEX16[i] = convert to hexadecimal
11:	***end for***
12	enc[i] = encrypt v[i] using SKHEX16 [i]
13	Save enc[i] in cloud database
14	Procedure: key re-generation and decryption (doctor's device)
15	***for***j = 1 to ndo
16	Repeat step 5 to 10
17	***end for***
18	dec[j] = decrypt v[j] using SKHEX16 [j]
19	END

6. Attack model

Widely induced attacks on secret key, such as Brute Force attack [51,52], Guessing attack [53,54], Birthday attack [55,56] are considered in this work.A brute force attack is a cryptanalytic attack which attempts to decrypt an encrypted data. An attacker can use a lot of possible secret keys to decrypt. A systematic way is followed to try all possible secret keys in the decryption process until the correct one is found. Attacker also attempts to get the key, which is derived from a password or secret value using Key Derivation Function, this is known as exhaustive key search.

The relation between key length and time is critical when it comes to the security of cryptographic algorithms [57]. The key space, which is determined by the length of the encryption key, directly affects the time required to perform a brute force attack on the encrypted data. Brute force attacks involve trying every possible combination of characters until the correct key is found, and the larger the key space, the more combinations that need to be tried, making the attack more time-consuming and computationally expensive. n symmetric encryption, the same key is used for both encryption and decryption. The key length directly determines the size of the key space. If the key length is denoted as "n" (in bits), the key space will have 2^n possible combinations. As a result, the time complexity of a brute force attack on symmetric encryption is proportional to 2^n.

In Guessing attack, a pattern of the key is known to attacker and using that patter attacker generates the set of keys. This set of keys is later used as dictionary in Brute Force Attack.This kind of attack is also known as Mask attack where attacker knows or assumes that the secret key pattern can be: 1. Length of secret key is 16, 2. Secret key contains alphabets and digits, 3. It contains 0–9 digits and A-F alphabets, 4. All are in Upper case. These information helps the attacker to reduce the number of possible combinations and hence cracking can be easy and faster.

The birthday attack leverages the birthday paradox, which states that in a set of n randomly chosen people, the probability that at least two people share the same birthday increases significantly when n is less than 23.In cryptographic terms, for a hash function with n possible outputs, finding two distinct inputs that hash to the same output (a collision) requires roughly $2^{n/2}$ attempts, rather than 2^n. The actual entropy of the key depends on the variability and range of the input components. Based on these three attacks cryptanalysis has been conducted and results have been discussed in later section.

6.1. Informal analysis

6.1.1. Theorem 1: secure from guessing attack

Assume that the attacker tries to guess the secret key SKHEX16. It is impossible to guess the SKHEX16 because the initial pattern of the key is [mm||HH||DD||MM||YYYY]. In this pattern key is changed in every minute because the mm element of the key sequence is changed in every minute while rest of elements of key sequence is unchanged for a time frame. To make it more complex DTIM has been converted to binary number and select left 32 bit from the BIN where BIN32 $\subset$ BIN. Final key SKHEX16 is formed by converting [BIN32|| BIN32′] to hexadecimal. So, a small change in the sequence differs the final key elements. Hence the attacker cannot guess the secret key. Therefore, the protocol is free from guessing attack.

6.1.2. Theorem 2: secure from brute force attack

Imagine a scenario where an attacker manages to intercept a message and decides to attempt to uncover the secret key by using a brute force approach. However, the security of the situation lies in the fact that the secret key, referred to as SKHEX16, is a 16-bit hexadecimal number. This translates to an incredibly large number of possible combinations – precisely 16 raised to the power of 16, which equals 18,446,744,073,709,551,616 (1.8 quintillion) unique secret keys.Given the astronomical number of potential secret keys, the process of trying each combination through brute force becomes unfeasible in practical terms. It would take an extensive amount of time, possibly spanning many years, to exhaustively search for the correct SKHEX16. Consequently, the protocol stands secure against brute force attacks due to the sheer implausibility of discovering the right key within a reasonable timeframe.

6.1.3. Theorem 3: secure from birthday attack

When discussing the security of a 64-bit key, it's essential to understand the amount of randomness, or "entropy," present in the key. The more entropy, the harder it is for someone to guess or crack the key. Our scheme uses several components from the date and time to build the key, and each of these components adds some entropy. Let's break down the entropy contribution of our proposed scheme for each component: mm (minute): 0–59 (6 bits), HH (hour): 0–23 (5 bits), DD (day): 1–31 (5 bits), MM (month): 1–12 (4 bits), YYYY (year): Assuming a reasonable range of 100 years (7 bits), Milliseconds (SSS): 0–999 (10 bits). Total bits of entropy $= 6 + 5 + 5 + 4 + 7 + 10 = 37$ bits, the birthday attack would require $2^{37/2} = 2^{18.5} \approx 370728$ attempts to find a collision. The validity period of 60 s means the key is valid only for a short window, reducing the risk of successful brute force or birthday attacks within that period.

6.2. Formal analysis

For guessing attack, all possible key sequence has been simulated using Matlab to check the best sequence for which the final key is very much different. For each sequence, 60 keys (range of mm is 00–59) has been generated and the average similarity has been calculated using eq (2). Table 2 shows the simulation results.

$$\text{Avarage similarity} = \frac{\textit{Total number of smilar characters}}{\textit{key length} \times {}^{n}_{2}C} \times 100 \tag{2}$$

Upon reviewing the provided table, a noticeable disparity in similarity emerges, indicating that sequence 1 exhibits a lower degree of similarity compared to the other sequences. Consequently, in the context of generating key sequences, if an attacker endeavors to produce successive keys based on a captured one, the probability of success is a mere 9.2 %. As a result, sequence 1 has been determined as the optimal choice for implementation within our key generation methodology.

The average similarity between keys generated by different sequences ranges from 9.2 % to 26.88 %. Lower similarity percentages indicate more distinct keys, which reduces the likelihood of collisions. To find a collision, an attacker would need to try approximately 370,728 different combinations. Given the 60-s validity window for each key, the practical feasibility of a birthday attack is very low.

Brute force tool called BruteX has been used to simulate brute force attack on the secret keys. A predefined time limit of 60 min was established for conducting the brute force experiment, as shown in Table 3. When dealing with a 28-bit key consisting of the elements YYYY, MM, and DD, we successfully cracked it in a mere 4 s. Moving to a 32-bit key containing YYYY, MM, and DD, the decryption was achieved in approximately 80 s. Similarly, 48-bit key utilizing analogous date components was deciphered within 58 min. However, it's noteworthy that a 64-bit key formed from mm, HH, DD, MM, and YYYY proved to be resistant to our efforts and couldn't be cracked within the set time threshold.In our scheme a key is valid for 60 s only. Thus, it is clear that our proposed key generation scheme is resilient to Brute Force Attack.

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.

7.1. Ethics declarations

This study was reviewed and approved by the Institutional Research Board of Maulana Abul Kalam Azad University of Technology. Members are Dr. Suparna Biswas, Dr. Ramesh Saha, and Dr. Koushik Karmakar.

All participants provided informed consent to participate in the study.

Table 2
Guessing attack simulation result for various sequence.

Sequence	Elements	Value	Key	Avg. Similarity
Seq-1	mmHHDDMMYYYY	151011102020	8CA3DA35735C25CA	9.2 %
Seq-2	mmDDHHMMYYYY	151110102020	8CBB74B073448B4F	12.66 %
Seq-3	HHmmDDMMYYYY	101511102020	BD1223F242EBBC0D	13.58 %
Seq-4	HHDDmmMMYYYY	101115102020	BC57701A43A88FE5	26.88 %
Seq-5	DDmmHHMMYYYY	111510102020	CFB42900304BD6EE	15.79 %
Seq-6	DDHHmmMMYYYY	111015102020	CEC820323137DFCD	26.88 %

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

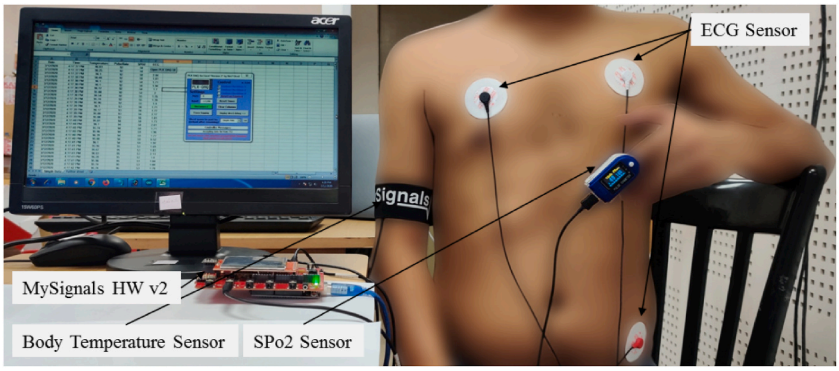
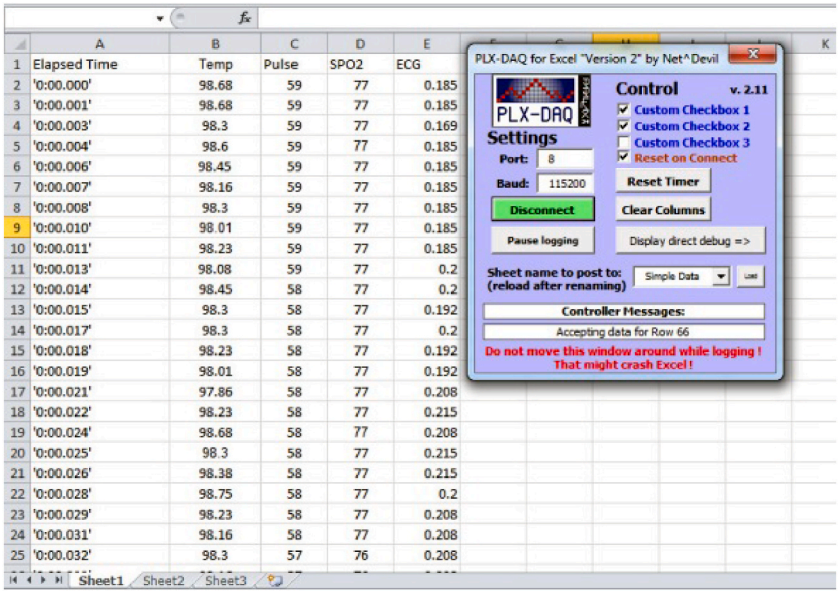


Fig. 4. IoMT based Experimental setup for health data collection.



	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

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

Screenshot of user interface for patient and doctor devices during data transmission has been shown in Fig. 6(a) and (b).

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 algorithm 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.

Data Read is the time required to read the sensor data from dataset, it takes an average time of 0.2–0.4 ms. Key generation is the time required to generate secret key by our proposed scheme which takes an average of time 2.20–2.80 ms.Encryption represents the

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

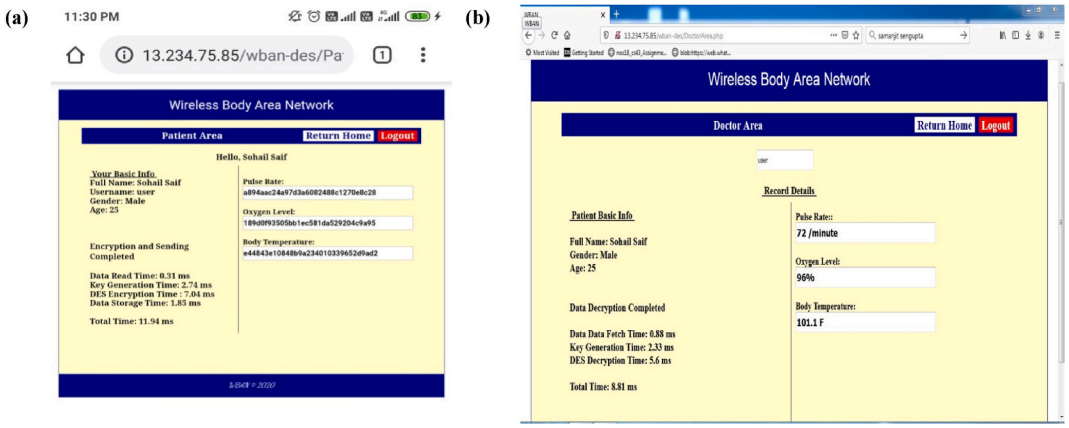


Fig. 6. User interface of patient and doctor device during data transmission.

time required to encrypt the health data such as Pulse Rate, Oxygen saturation level and Body temperature. Experimental results show that it takes an average of 5.20–6.03, 6.19–7.24 and 6.56–7.26 ms for ECB, CBC and CTR mode respectively. Data Save represents the time incurred to store the encrypted health data in AWS server.Similarly, Data Retrieve is the time component involved in retrieval of encrypted data from cloud database to doctors' device. Both of these operations take an average time of 1.50–2.12 ms and 0.85–1.01 ms.Key re-generation depicts the time experienced for secret key generation at doctor's device using the same scheme, it takes an average of 2.29–2.94 ms. Decryption is the time required to decrypt the encrypted health data into meaning full plain text. Average decryption time required by ECB, CBC and CTR modes are 4.20–5.06 ms, 5.09–6.23 ms and 5.17–6.03 ms respectively. There is a significant increase of time for CBC and CTR mode compared to ECB due to the complex nature. Total time is the sum of the time required by all above mentioned operations to complete 1 transmission, it has been observed that for ECB,CBC and CTR modes average total transmission time lies between 17.73 and 19.34 ms, 19.38–21 ms and 20.05–21.39 ms respectively. Table 5 shows the comparison with a similar approach proposed by Hamid et al. [59], It can be seen from the table that our approach is 87 % faster than the compared one.

Since our key generation scheme is based on system time and date, the most changing element is mm, it is changed in every minute thus the key is changed. This change can lead to generation of wrong key at doctors' device for the same transmission. For example, a key is generated on patient's device at 28 min past 3′O clock, where the system date time was 03:28:59:995, but when it reaches at doctor's device the time becomes 03:29:00:017, so doctor's device will generate a different key based on this information which will lead to failure of decryption process. There could be a maximum 1 failure in a minute using our key generation scheme due to change in clock. The total number of encryptions per minute, as well as decryptions, are recorded to indicate the number of failures. The difference between these two values represents the number of failures.Fig. 8(a) and (b) and (c) shows the total number of transmissions for three modes.

Out of 60 min, at 1st minute 3240 transmissions has been encrypted and transmitted but 3239 transmissions have been successfully decrypted, hence 1 transmission has been discarded due to invalid decryption key. Similarly at the 7th minute total number of encrypted, transmitted and decrypted transmission is 3236, hence no failure is present. It can be observed that an average of 3236–3243 numbers of transmissions has been successfully encrypted and decrypted during transmission in DES-ECB mode. For DES-CBC mode the numbers of successful encrypted and decrypted transmission lies between 2967 and 2975, which is less than ECB mode, since total time required for each transmission is more than ECB mode. Similarly, in DES-CTR mode it can be discovered that 2858–2863 transmissions has been completed each minute which is less than other two modes due since time required for a each transmission is more than other two modes.In Fig. 9 percentage of packet delivery ratio per minute for all three modes have been shown.To calculate the packet delivery ratio equation (3) has been used.

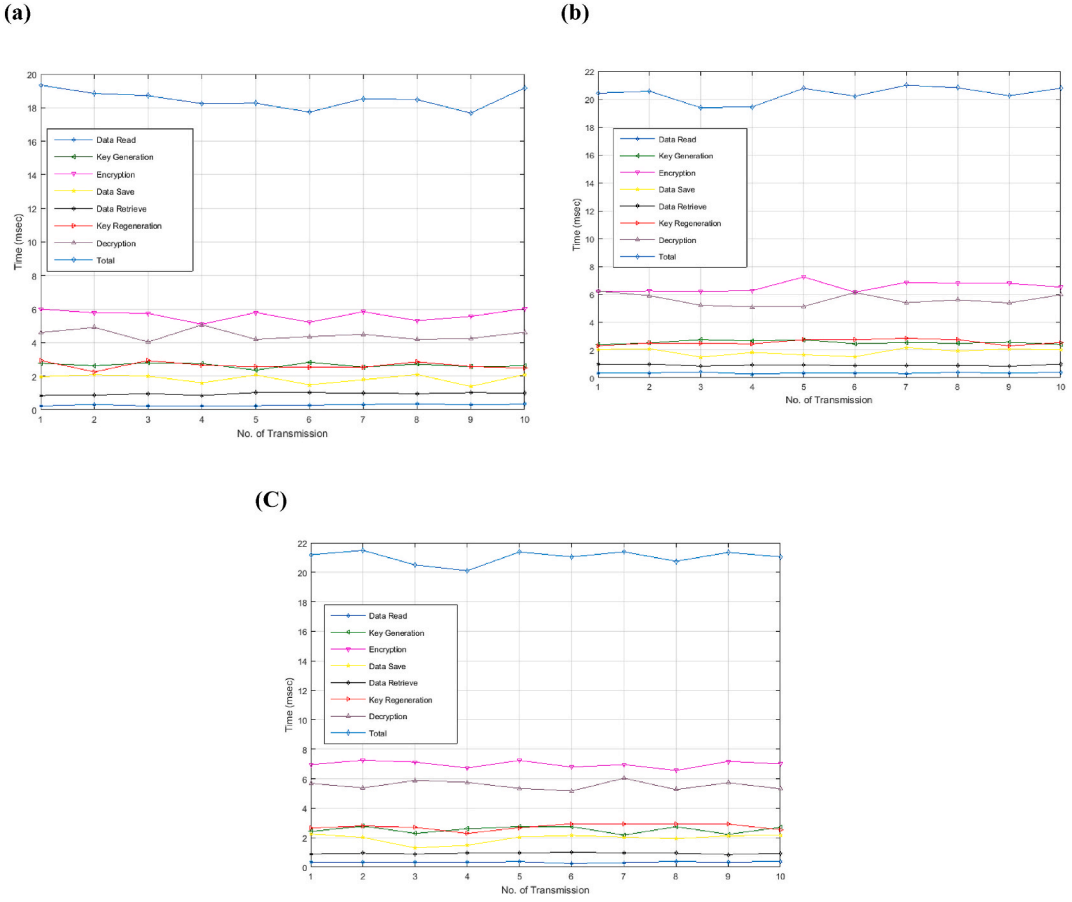


Fig. 7. Time required during secure data transmission in **a.** DES-ECB mode **b.**DES-CBC mode **c.**DES-CTR mode.

Table 5
Comparison with related work in terms of key generation and encryption/decryption time.

Authors	Approach	Key Generation Time	Encryption/Decryption Time	Total Time
Hamid et al. [59]	ECC (106 bits)	57 ms	11 ms	68 ms
	ECC (132 bits)	98 ms	17 ms	115 ms
	ECC (160 bits)	108 ms	16 ms	124 ms
	ECC (210 bits)	121 ms	15 ms	136 ms
	RSA (512 bits)	383 ms	77 ms	460 ms
	RSA (768 bits)	898 ms	160 ms	1058 ms
	RSA (1024 bits)	2609 ms	338 ms	2947 ms
	RSA (2048 bits)	18399 ms	1867 ms	20266 ms
Proposed	DES-ECB (64 bits)	2.8 ms	6.03 ms	8.83 ms
	DES-CBC (64 bits)	2.8 ms	7.24 ms	10.04 ms
	DES-CTR (64 bits)	2.8 ms	7.26 ms	10.06 ms

$$\text{Packet delivery ratio} = \frac{\textit{succesfully received and decrypted packets}}{\textit{total number of packets encrypted and transmitted}} \times 100 \tag{3}$$

Above figure shows that on 7th,25th, 42nd, 59th minute DES-ECB mode has achieved 100 % of packet delivery ratio, for the rest of the minutes the percentage lies between 99.95 and 99.97 %. For DES-CBC mode percentage of packet delivery ratio for 60 min lies between 99.93% and 99.94 % and for DES-CTR mode 8th, 19th and 23rd minutes has obtained 100 % of packet delivery ratio, for the rest of the minutes the percentage lies between 99.92 and 99.93 %. Table 6 Shows the total number of packets encrypted, successful decryption and failed decryption during 60 min of transmission.

Fig. 10 states the comparison with similar works conducted in last few years. From the above results it can be seen that DES-ECB mode obtains the highest rate of packet delivery and it reduces the chance of failed decryption. Also as discussed earlier this mode takes 17.73–19.34 ms for one, which is within the permissible limit in healthcare [60–62]. This makes it suitable to be applied in healthcare

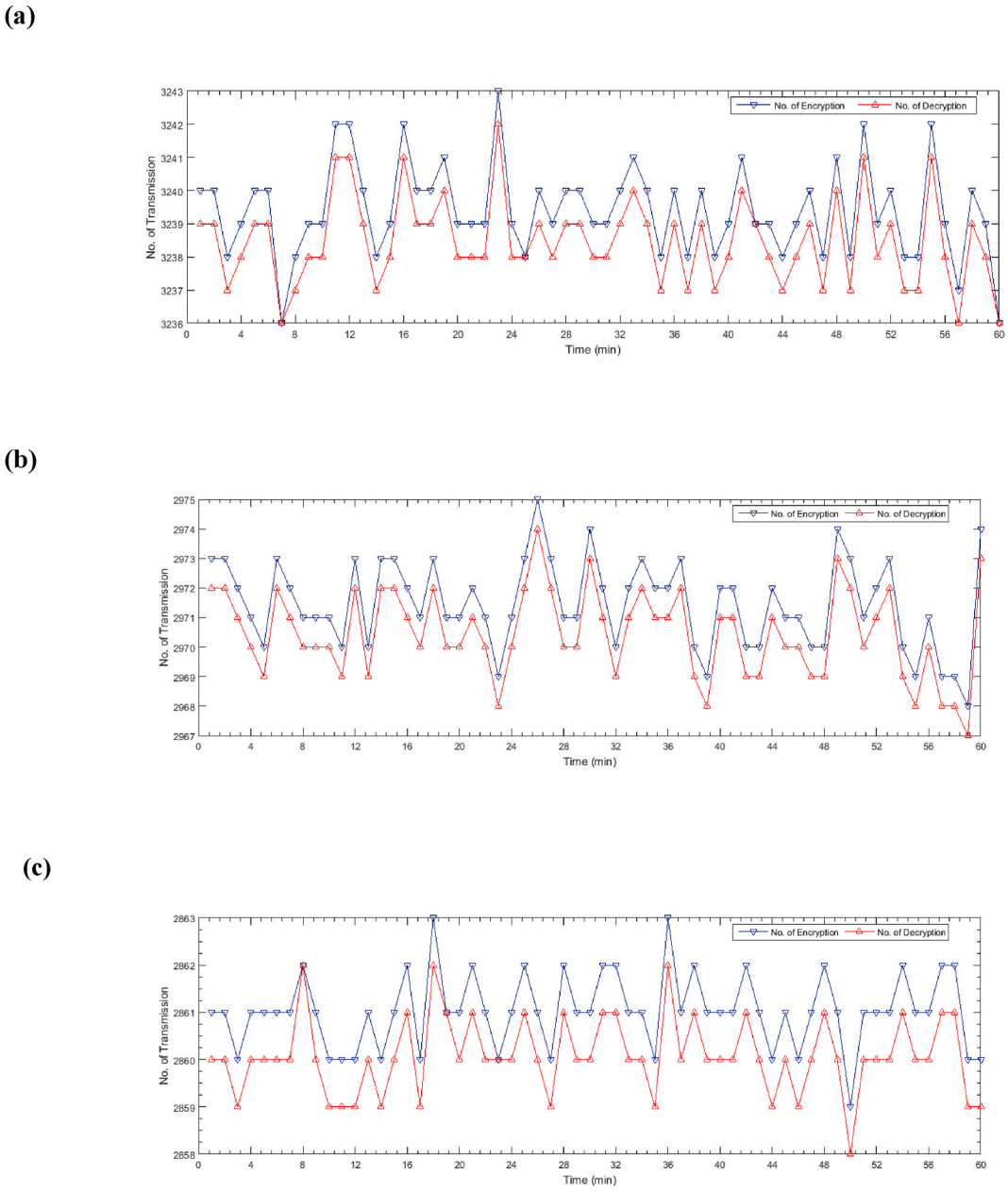


Fig. 8. Encryption and Decryption during data transmission **a.** DES-ECB mode **b.**DES-CBC mode **c.**DES-CTR mode.

applications to ensure confidentiality of health data.

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. Results showed transmission times ranging from 17.73 to 21.39 ms and packet transmission rates of 3236 to 2858 packets per minute for DES-

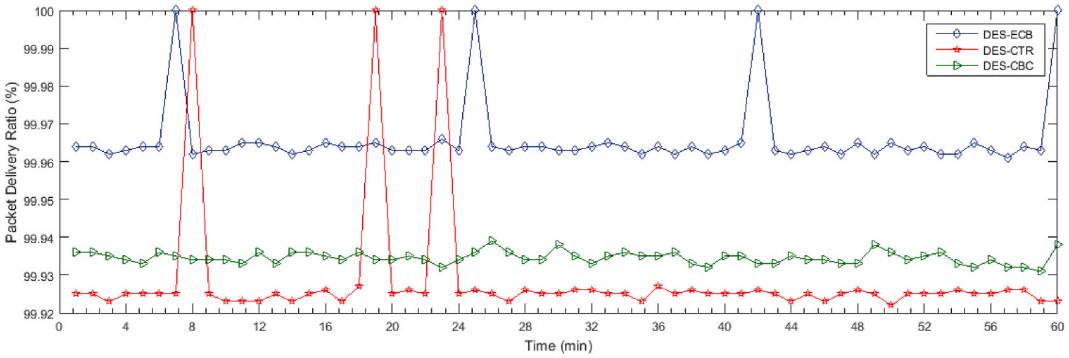


Fig. 9. Percentage of Packet Delivery Ratio for all three modes.

Table 6
Packets transmitted from patients' to doctors' device in 60 min.

Mode	Total Encrypted Packet	Successful Decrypted Packet	Un Successful Decryption
DES-ECB	194364	194308	56
DES-CBC	178288	178228	60
DES-CTR	171662	171605	57

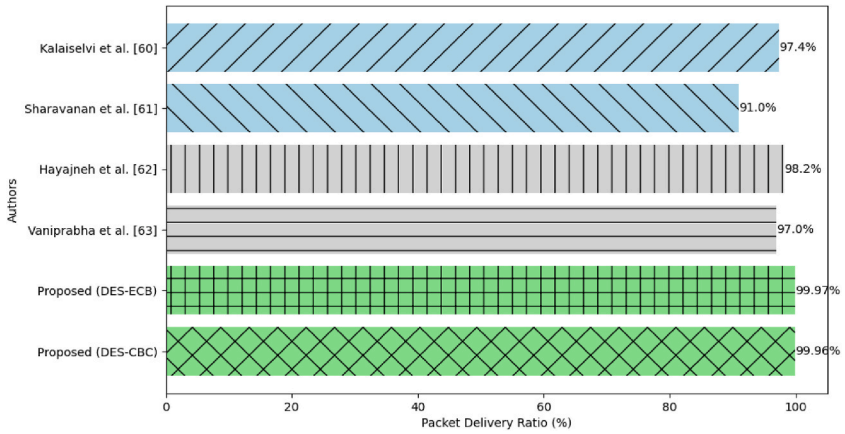


Fig. 10. Comparison with related works in terms Packet delivery ratio.

ECB, DES-CBC, and DES-CTR modes, respectively.

Despite these advancements, limitations exist. Our focus on common security attacks may overlook emerging threats, and reliance on the DES algorithm warrants exploration of alternative cryptographic methods. Additionally, accommodating the growing volume and diversity of health data poses scalability challenges. Future research could explore advanced threat models, algorithmic enhancements, and real-world deployment studies to address these limitations.

Conflicts of interest/Competing interests

Authors of this manuscript declare that they have no conflict of interest.

Availability of data and material

The datasets generated and/or analyzed during the current study are not publicly available due to privacy of the subjects but are available from the corresponding author on reasonable request.

CRediT authorship contribution statement

Sohail Saif: Writing – review & editing, Writing – original draft, Visualization, Software, Methodology, Investigation, Formal

analysis, Conceptualization. **Priya Das:** Writing – review & editing, Writing – original draft, Visualization, Software, Methodology, Investigation, Formal analysis, Conceptualization. **Suparna Biswas:** Writing – review & editing, Writing – original draft, Validation, Software, Methodology, Investigation, Formal analysis, Conceptualization. **Shakir Khan:** Writing – review & editing, Visualization, Validation, Methodology, Data curation. **Mohd Anul Haq:** Writing – review & editing, Validation, Software, Data curation. **Viacheslav Kovtun:** Validation, Supervision, Resources, Project administration, Funding acquisition, Data curation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

The authors are grateful to all colleagues and institutions that contributed to the research and made it possible to publish its results.

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.
[12] S. Saif, R. Gupta, S. Biswas, A complete secure cloud-based WBAN framework for health data transmission by implementing authenticity, confidentiality and integrity, Int. J. Adv. Intell. Paradigms 20 (1–2) (2021) 171–189.
[13] S. Saif, S. Biswas, Secure data transmission beyond tier 1 of medical body sensor network, in: Proceedings of International Ethical Hacking Conference 2018: eHaCON 2018, Springer, Kolkata, India, 2019, pp. 405–417. Singapore.
[14] W. Wang, Q. Chen, Z. Yin, G. Srivastava, T.R. Gadekallu, F. Alsolami, C. Su, Blockchain and PUF-based lightweight authentication protocol for wireless medical sensor networks, IEEE Internet Things J. 9 (11) (2021) 8883–8891.
[15] S. Saif, P. Das, S. Biswas, M. Khari, V. Shanmuganathan, HIIDS: hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in IoT based healthcare, Microprocess. Microsyst. 104622 (2022).
[16] S. Saif, N. Mondal, S. Biswas, Secure electronic health record storage and retrieval using blockchain and encryption for healthcare application, SN Computer Science 4 (3) (2023) 300.
[17] M.K. Hasan, M. Shafiq, S. Islam, B. Pandey, Y.A. Baker El-Ebiary, N.S. Nafi, D.E. Vargas, Lightweight cryptographic algorithms for guessing attack protection in complex internet of things applications, Complexity (2021).
[18] M. Adil, M.K. Khan, M.M. Jadoon, M. Attique, H. Song, A. Farouk, An AI-enabled hybrid lightweight authentication scheme for intelligent IoMT based cyber-physical systems, IEEE Transactions on Network Science and Engineering (2022).
[19] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, R. Jain, Recent advances in the internet-of-medical-things (IoMT) systems security, IEEE Internet Things J. 8 (11) (2020) 8707–8718.
[20] N. Garg, M. Wazid, J. Singh, D.P. Singh, A.K. Das, Security in IoMT-driven smart healthcare: a comprehensive review and open challenges, Security and Privacy 5 (5) (2022) e235.
[21] G. Margelis, X. Fafoutis, G. Oikonomou, R. Piechocki, T. Tryfonas, P. Thomas, Efficient DCT-based secret key generation for the Internet of Things, Ad Hoc Netw. 92 (2019) 101744.
[22] A. Soni, R. Upadhyay, A. Kumar, Performance improvement of wireless secret key generation with colored noise for IoT, Int. J. Commun. Syst. 32 (16) (2019) e4124.
[23] L. Chen, K. Cao, T. Lu, Y. Lu, A.A. Hu, one-time pad encryption scheme based on efficient physical-layer secret key generation for intelligent IoT system, China Communications 19 (7) (2022) 185–196.
[24] J. Tang, H. Wen, H.H. Song, L. Jiao, K. Zeng, Sharing secrets via wireless broadcasting: a new efficient physical layer Group secret key generation for multiple IoT devices, IEEE Internet Things J. (2022).
[25] M. Usman, S. Althunibat, M. Qaraqe, A channel state information-based key generation scheme for internet of things, Secur. Commun. Network. (2022).
[26] K.K. Coelho, M. Nogueira, M.C. Marim, E.F. Silva, A.B. Vieira, J.A.M. Nacif, LORENA: low memORysymmEtric-key geNerAtion method for based on Group cryptography protocol applied to the internet of healthcare things, IEEE Access 10 (2022) 12564–12579.
[27] S. Das, S. Namasudra, A novel hybrid encryption method to secure healthcare data in IoT-enabled healthcare infrastructure, Comput. Electr. Eng. 101 (2022) 107991.
[28] M. Kumar, S. Verma, A. Kumar, M.F. Ijaz, D.B. Rawat, ANAF-IoMT: a novel architectural framework for IoMT-enabled smart healthcare system by enhancing security based on RECC-VC, IEEE Trans. Ind. Inf. 18 (12) (2022) 8936–8943.
[29] S.A. Sultana, R. Ch, R.P. Malleswari, Keyless lightweight encipher using homomorphic and binomial coefficients for smart computing applications, in: 2023 2nd International Conference on Vision towards Emerging Trends in Communication and Networking Technologies (ViTECoN), IEEE, 2023, May, pp. 1–6.

[30] J. Iqbal, H. Bibi, N.U. Amin, H. AlSalman, S.S. Ullah, S. Hussain, N. Al-Aidroos, Efficient and secure key management and authentication scheme for WBSNs using CP-abe and consortium blockchain, J. Sens. (2022).
[31] A. Kumar, S. Sharma, N. Goyal, A. Singh, X. Cheng, P. Singh, Secure and energy-efficient smart building architecture with emerging technology IoT, Comput. Commun. 176 (2021) 207–217.
[32] C. Rupa, D. MidhunChakkarvarthy, R. Patan, A.B. Prakash, G.G. Pradeep, Knowledge engineering–based DApp using blockchain technology for protract medical certificates privacy, IET Commun. 16 (15) (2022) 1853–1864.
[33] R. Ch, G. Srivastava, T.R. Gadekallu, P.K.R. Maddikunta, S. Bhattacharya, Security and privacy of UAV data using blockchain technology, J. Inf. Secur. Appl. 55 (2020) 102670.
[34] R. Ch, Squint pixel steganography: a novel approach to detect digital crimes and recovery of medical images, Int. J. Digital Crime Forensics (IJDCF) 8 (4) (2016) 37–47.
[35] Y.M. Tseng, T.C. Ho, T.T. Tsai, S.S. Huang, AHMRE-SCST: lightweight anonymous heterogeneous multi-recipient encryption with seamlessly compatible system transformation for IoT devices, IEEE Internet Things J. (2024).
[36] L. Pu, C. Lin, B. Chen, D. He, User-friendly public-key authenticated encryption with keyword search for industrial internet of things, IEEE Internet Things J. (2023).
[37] M. Usman, S. Althunibat, M. Qaraqe, A channel state information-based key generation scheme for Internet of Things, Secur. Commun. Network. 2022 (2022).
[38] D. Guo, K. Cao, J. Xiong, D. Ma, H. Zhao, A lightweight key generation scheme for the internet of things, IEEE Internet Things J. 8 (15) (2021) 12137–12149.
[39] M. Jacovic, M. Kraus, G. Mainland, K.R. Dandekar, Evaluation of physical layer secret key generation for IoT devices, in: 2019 IEEE 20th Wireless and Microwave Technology Conference (WAMICON), IEEE, 2020, April, pp. 1–6.
[40] Fatemeh Pirmoradian, Masoumeh Safkhani, Seyed Mohammad Dakhilalian, ECCPWS: an ECC-based protocol for WBAN systems, Comput. Network. 224 (2023) 109598.
[41] M. Soni, D.K. Singh, New directions for security attacks, privacy, and malware detection in WBAN, Evolutionary Intelligence 16 (6) (2023) 1917–1934.
[42] M. Luo, Y. Pei, M. Qiu, Cross domain heterogeneous signcryption scheme with equality test for WBAN, Wireless Pers. Commun. 130 (2) (2023) 1107–1122.
[43] A.S. Rajasekaran, M. Azees, C.S. Dash, A. Nayyar, Content addressable memory (CAM) based robust anonymous authentication and integrity preservation scheme for wireless body area networks (WBAN), Multimed. Tool. Appl. (2023) 1–27.
[44] D. Rangwani, H. Om, Four-factor mutual authentication scheme for health-care based on wireless body area network, J. Supercomput. (2022) 1–35.
[45] S. Izza, M. Benssalah, K. Drouiche, An enhanced scalable and secure RFID authentication protocol for WBAN within an IoT environment, J. Inf. Secur. Appl. 58 (2021) 102705.
[46] A. Kumar, S. Sharma, N. Goyal, S.K. Gupta, S. Kumari, S. Kumar, Energy-efficient fog computing in internet of things based on routing protocol for low-power and lossy network with contiki, Int. J. Commun. Syst. 35 (4) (2022) e5049.
[47] V. Kumar, V. Pathak, N. Badal, P.S. Pandey, R. Mishra, S.K. Gupta, Complex entropy-based encryption and decryption technique for securing medical images, Multimed. Tool. Appl. 1–19 (2022).
[48] P.N. Srinivasu, A.K. Bhoi, S.R. Nayak, M.R. Bhutta, M. Woźniak, Blockchain technology for secured healthcare data communication among the non-terminal nodes in IoT architecture in 5G network, Electronics 10 (12) (2021) 1437.
[49] R. Jeet, S.S. Kang, S.M. Safiul Hoque, B.N. Dugbakie, Secure model for IoT healthcare system under encrypted blockchain framework, Secur. Commun. Network. (2022).
[50] R. Kumar, P. Khan, S. Kumar, Healthcare data encryption technique using hybrid cellular automata in IoT networks, Wireless Pers. Commun. 1–19 (2022).
[51] C. Tezcan, Key lengths revisited: GPU-based brute force cryptanalysis of DES, 3DES, and PRESENT, J. Syst. Architect. 124 (2022) 102402.
[52] M. Mitev, A. Chorti, E.V. Belmega, H.V. Poor, Protecting physical layer secret key generation from active attacks, Entropy 23 (8) (2021) 960.
[53] M.R. Senouci, I. Benkhaddra, A. Senouci, F. Li, An efficient and secure certificateless searchable encryption scheme against keyword guessing attacks, J. Syst. Architect. 119 (2021) 102271.
[54] Y. Zhong, J.H. Feng, X.X. Cui, X.L. Cui, Machine learning aided key-guessing attack paradigm against logic block encryption, J. Comput. Sci. Technol. 36 (5) (2021) 1102–1117.
[55] G.T. Chavan, S. Agrawal, N.N. Sakhare, D. Mondal, M. Vigenesh, G. Vijayalakshmi, Investigating the effectiveness of birthday attack strategies in cryptography network security, in: 2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), IEEE, 2023, December, pp. 1–6.
[56] F. Ullah, C.M. Pun, Deep self-learning based dynamic secret key generation for novel secure and efficient hashing algorithm, Inf. Sci. 629 (2023) 488–501.
[57] C. Rupa, M.A. Shah, Novel secure data protection scheme using Martino homomorphic encryption, J. Cloud Comput. 12 (1) (2023) 1–12.
[58] S. Saif, R. Saha, S. Biswas, On Development of MySignals based prototype for application in health vitals monitoring, Wireless Pers. Commun. 122 (2) (2022) 1599–1616.
[59] H.A. Al Hamid, S.M.M. Rahman, M.S. Hossain, A. Almogren, A. Alamri, A security model for preserving the privacy of medical BigData in a healthcare cloud using a fog computing facility WithPairing-based cryptography, IEEE Access 5 (2019) 22313–22328.
[60] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, A. Jamalipour, Wireless body area networks: a survey, IEEE Communications Surveys & Tutorials 16 (3) (2014) 1658–1686.
[61] J. Khan, G.A. Khan, J.P. Li, M.F. AlAjmi, A.U. Haq, S. Khan, A. Ali, Secure smart healthcare monitoring in industrial internet of things (iiot) ecosystem with cosine function hybrid chaotic map encryption, Sci. Program. 2022 (1) (2022).
[62] S. Ahmad, S. Khan, M.F. AlAjmi, A.K. Dutta, L.M. Dang, G.P. Joshi, H. Moon, Deep learning enabled disease diagnosis for secure internet of medical things, Comput. Mater. Continua (CMC) 73 (1) (2022).