NJESR/ March-2023/Volume-5/Issue-3 E-ISSN-2582-5836
DOI-10.53571/NJESR.2023.5.3.65-75

Security Of Data Transmission In Remote Health Care Monitoring System

Sreevidya V.S
Lecturer In Computer Engineering,
Government Polytechnic College
Punalur

(Received:25 Feburary2023/Revised:14March2023/Accepted:20March2023/Published:30March2023)

Abstract

In healthcare applications with biosensor collections connected to a human body or in an emergency care unit, wireless medical sensor networks are used to monitor the physiological vital status of the patient. A diagnostic center receives the real-time medical data gathered by wearable medical sensors. At this center, the data from the sensors are combined and sent to the doctor's personal digital assistant for further analysis. Unauthorized access to a person's health data may result in misuse and legal complications, and patients may be put in danger if the data is transmitted or stored in an unreliable manner. As a result, in order to safeguard the medical sensor network's access control system and data transmission, this letter combines attribute-based encryption with a symmetric algorithm. In this work, the best performance is determined by comparing existing systems and their algorithms. The work likewise shows the graphical correlation of encryption time, unscrambling time and complete calculation season of the current and the proposed frameworks.

Keywords: Secured Remote Health Monitoring System, Wireless Medical Sensor Network, Symmetric Algorithm, Attribute-Based Encryption, Data Transmission

Introduction

In the current research, a new technology known as a wireless sensor network (WSN) promises to make human life easier. The smallest component of a network is a wireless sensor, which is utilized in numerous applications like the armed forces, water irrigation, soil moisture testing, structural health monitoring, field monitoring, volcanic activity monitoring, and monitoring of human health care, among others.

WSNs' recent advancements have led to a plethora of healthcare applications. It has made another field of remote clinical sensor organizations (WMSNs). Human health can be tracked and monitored with any of the biosensors that can be worn or not worn. The WMSN is used to record the patient's health status and monitor the sportsperson's health activities[1]. The patient

requires continuous health monitoring, either in a hospital or at home. The diagnostic center receives the biosensor-collected data via a wireless network. Attacks are possible when health data is sent through wireless networks. The individual's data may be misused by others during transmission, posing a threat to the individual's life[2]. As a result, healthcare applications are fundamentally dependent on security.

The security components applied in customary organization can't be applied to WMSN on account of the asset imperatives of sensor network[3] like low computational limit, battery fueled gadget, and broadcast correspondence in nature, however WMSN's security needs are equivalent to that of regular organizations concerning network accessibility, credibility, secrecy, information newness and uprightness. Medical data security has been a topic of discussion among numerous researchers. Some of the works have only contributed to data authentication, while others have focused solely on data integrity and confidentiality[4]. The encryption algorithm and access control mechanisms of the proposed secured remote health monitoring system (SHS) are combined to guarantee the integrity, authenticity, and confidentiality of data.

The examined medical data are securely transmitted to the diagnostic center's server via blowfish encryption in this work. At this center, the data from the sensors are combined and sent to the doctor's personal digital assistant (PDA). The information from the analytic focus should be gotten to by the approved specialists, attendants and experts in emergency clinics. As a result, the attribute-based encryption (ABE) algorithm is utilized across the network as well. If a patient's data shows an abnormality, healthcare professionals at the center will quickly respond to the patient's emergency and send an ambulance and medical personnel to the patient's location to save their lives. By comparing the proposed system to other approaches of a similar nature, the experimental results demonstrate the system's effectiveness.

Information On Related Works

A novel, lightweight method for protecting WMSNs has been proposed in[5], and it consists of four parts: i) the system initialization segment, in which the network server creates a medical sensor network (MSN), ii) the user joining segment, in which the user can use commands to interact with the MSN, iii) the regular user segment, in which the medical data from each biosensor node is sent to the network server through the controller (for mobile phones), and iv) the user command segment, in which the network user can create a new command and send it to the network server using the Using the one-way hash function message digest 5 (MD5) and the

encryption algorithm advanced encryption standard (AaES), the system ensures secure transmission and access control. Because it does not make use of any verification tables on the server, it uses less power and storage space.

The data that is collected by the medical sensors is divided into three components and stored in three distributed servers in order to provide security for both the data store and the data access [6]. For instance, the sensed medical data is broken down into three integers, so that + + + = Personal identification attributes and these values are stored in three distributed servers S1, S2, and S3 under the names "Ai, i," "Ai, i," and "Ai, i," respectively. The digital signature and the Paillier cryptosystem are used to control who can access the medical data and keep it private. The method has the advantage of being safe from both outside and inside attacks because it uses distributed servers, and the value of can only be calculated with knowledge of and values.

Personal health information can be safeguarded using biological traits as an alternative to cryptographic methods. The biometric approach is used to secure the keys and identify sensor motes in the network in the system[7]. ECG and photoplethysmogram signals are used to calculate the heartbeat's inter-pulse interval (IPI). The binary entity identifier, which is used to identify the sensor motes in the body sensor network, is generated from the IPI.

The patient's physiological signals, such as the ECG signal, glucose level, blood pressure, and body temperature, are monitored by the body sensor nodes in[8]. Bluetooth is used to send these readings to the patient's PDA. Steganography is used to conceal the patient's information in the PDA. Consequently, an internet-based watermarked ECG signal is sent to the hospital. Data authentication is provided by the system, which means that authorized doctors can only access the patient's information and watermarked signals.

There are three levels of network architecture in[9]. i) The wearable sensor network monitors physical information in the sensor network tier. ii) The versatile registering network level comprises of PDA and PC to course the clinical information to the remote base station or server. (iii) The back-end network tier is made up of servers and fixed stations that process the sensed data from mobile computing devices and store it for use in the future. The Bluetooth secure convention and public key foundation based cryptography are used to get the transmission of information among the sensor hubs, portable hubs and waiter.

The body area network transmits the body parameters or movements to the data sink (a mobile device) in[10]. There are four steps in the system: The system initialization that shares the master

key and public parameters with all network nodes is presented in step 1. If the user attributes satisfy the access tree, the private keys generated in Step 2 will be used to decrypt the ciphertext. Step 3 uses AES to encrypt the message and ciphertext policy ABE (CP-ABE) to encrypt the session key. Data consumers (doctors and nurses) decrypt the data in step 4 to obtain a session key, which they then use to decrypt the ciphertext. The method has a higher storage and computation cost, but the system protects data consumers, data sinks, and sensors.

Literature Overview

Over the past two decades, extensive research has been carried out in the field of healthcare to identify an effective method for data collection and transmission. Patches of various kinds were used in the developed monitoring systems to collect healthcare signal. Not only are the systems designed for patients with chronic conditions, but also for those in critical situations. There are many different health conditions that patients should have monitored in real time. For instance, wearable body sensor networks for monitoring blood pressure were suggested in[2]. In [3], a low-power, cost-effective wireless ECG monitoring system was developed that could be worn. Utilizing smartphones, healthcare systems that monitor diabetic patients were developed in[5]. In the writing[6], a remote checking framework was proposed to direct patients fostering Alzheimer's sickness by following their development examples and areas. A similar errand was carried out in[7] utilizing ZigBee. Additionally, a wearable monitoring system was developed to analyze the respiratory rate of patients in order to monitor the quality of their sleep[8],[9] conducts a survey of the various wearable technologies and monitoring systems available to Parkinson's disease patients.

Fix gadgets are implanted in patients' bodies. Therefore, it must be ensured that the integration of the device does not impede a patient's natural movements. Additionally, healthcare signals must be transmitted error-free at low power. Researchers use a wide range of low-power devices to transmit healthcare data to another processing unit. Due to its wide availability, resistance to challenges, and straightforward protocol structure, Bluetooth was the most widely used[7]. BLE, a new technology with a moderate communication range and low power consumption, has taken the place of Bluetooth. In the meantime, additional technologies based on radio frequency (RF) are being developed and used for remote health monitoring. For instance, a study was directed zeroing in on 6LowPAN-based remote observing[10]. Versatility the board has had the need in the writing. The literature[2] also contains a discussion of mobility support with 6LoWPAN. Remote

monitoring systems based on ZigBee and ANT have also been reported[3]. A smartphone or a personal computer (PC) can be used to process the signals that have been collected.

It is important to note that the interference from nearby devices can cause the aforementioned systems to experience a significant amount of BER[31,44]. Furthermore, the cell phone based administration frameworks are not extremely powerful in situations where the checking individual lives in another room or nowhere near the patient. Most investigations don't zero in on escalated care situations. When the connection's reliability is questioned, this kind of environment could mean the difference between life and death. Table 2 demonstrates that the majority of monitoring systems place a particular emphasis on low-power devices. However, new approaches to increasing reliability have not yet been proposed. For intensive care settings, a system with a focus on low power, low cost, high security, and improved reliability must be developed.

Performance Comparison Of Symmetric Key Algorithms

When compared to asymmetric key algorithms, symmetric key algorithms have a much smaller key size, use less memory, and take less time to compute. Additionally, because the medical data would only be communicated to a small number of users, such as patients' families and technicians, symmetric key algorithms are suitable for communication between a small number of users[11]. In SHS, the best algorithms for protecting medical data's privacy are symmetric algorithms.

Asymmetric key algorithms use different keys for encryption and decryption, whereas symmetric key encryption uses the same key for both. Further subdivided into two categories are the symmetric key algorithms: cipher for the block and stream[12] Bit by bit, stream ciphers typically employ distinct keys for each bit of encryption. The same key is used to encrypt each block of data or files (ranging in size from 64 to 128 bits) using the block ciphers[13]. The patient's health information is sent to the hospital as a block or file after being monitored for some time. Using symmetric block cipher, medical data are encrypted in SHS.

Performance comparisons are made between AES, DES, Rivest's cipher 6, RC6, blowfish, and the International data encryption algorithm (IDEA), which are the most common symmetric algorithms. The algorithms that are applied to the dataset referred to in [14] are implemented using Java. There are 130 observations in the dataset, and three variables—normal body temperature, gender, and heart rate—are included. The total computation time, the cost of

decryption, and the cost of encryption are used to compare the performance of symmetric algorithms.

The encryption time is shown in Table 1, the decryption time is shown in Table 2, and the total algorithmic computation time, which includes the time spent generating keys and encrypting and decrypting data, is shown in Table 3. According to the performance analysis, the blowfish algorithm has significantly lower encryption and decryption costs than the other algorithms. The blowfish algorithm is used in SHS to protect privacy because medical data must be transferred quickly.

Proposed System

A patient's body can be connected to one or more sensors, such as a heart rate sensor, a blood pressure sensor, an electrocardiogram (ECG) sensor, or a body temperature sensor, depending on the need. Before being sent, the sensor data on the common controller unit (a mobile phone) is encrypted with the blowfish algorithm. The encrypted information can be transmitted to the diagnostic center via Wi-Fi or 3G technology. At this center, the data from the sensors are compiled. The diagnostic center creates the database, which can help keep track of the patient's information and keep an eye on their health. The authorized doctors, nurses, and technicians can access the medical data using the ABE technique. The ambulance will fly to the patient's location using the global positioning system if the patient's diagnosis is abnormal. The proposed framework is outlined in Fig. 1.

Experimental results

SHS is implemented using the Net Beans IDE over the dataset referred in [1-4]. The performance comparisons are carried out on the basis of encryption time, decryption time and total computation time for the algorithms in[5, 6, 10].

Table 4 shows the encryption time for combinations of different algorithms. Among all the four methods, Paillier cryptosystem and digital signature consume more encryption time[6] as they split the data and do encryption three times at all the three distributed servers and again they have to perform decryption. So, the decryption time and eventually total computation time are higher compared with the other algorithms.

Table 5 shows the unscrambling season of the relative multitude of four mixes of calculations. Because the session key is encrypted and decrypted prior to the actual message encryption and decryption, CP-ABE and AES have a higher encryption and decryption cost than MD5 and AES.

When compared to the AES and MD5 algorithms, this uses a lot of storage space and costs a lot to compute. The algorithms' total computation times are shown in Table 6. When compared to the other algorithms, the Blowfish and CP-ABE algorithms used in SHS take significantly less time to compute. The medical information needs to get to the doctors and other medical professionals quickly. The blowfish algorithm is superior to any other algorithm combination due to its extremely low computation cost. The CP-ABE algorithm is also used to give users access control at the same time. The blowfish and CP-ABE algorithms are combined in SHS to provide medical data with privacy and access control.

Conclusion

The patient's physiological data are sensed by the medical sensor and transmitted via wireless channels, which are more susceptible than wired networks. Compared to symmetric key algorithms, the computational demands of public key algorithms are higher. Besides, they are not reasonable for sending short messages. As a result, the performance of symmetric key algorithms like AES, DES, blowfish, RC6, and IDEA is compared. Because of its good performance, the blowfish algorithm is used to encrypt medical data. The information should be gotten to exclusively by the approved clients with explicit control thus the CP-ABE is executed. Because it transmits medical data more quickly and with greater security than the other systems currently in use, the combination of these two algorithms is ideal for use in healthcare applications.

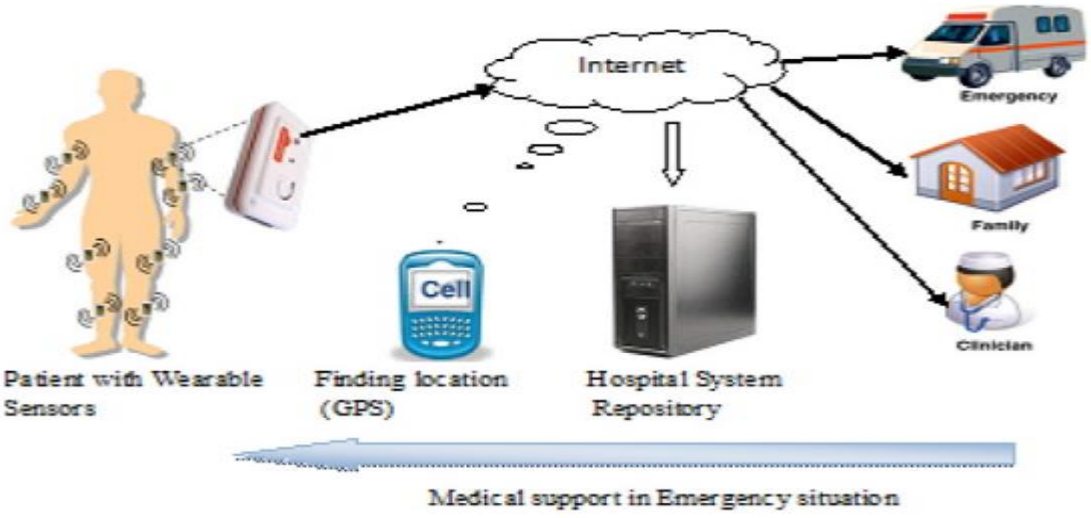

Fig. 1: Model Of The Proposed System

Table 1: Encryption Time Of Symmetric Algorithms

	51 kB	**204 kB**	**407 Kb**	**1531 kB**
AES, s	1	2	3	8
DES, s	0.5	0.98	2	7
blowfish, s	0.23	0.67	1.5	3
RC6, s	20	55	123	233
IDEA, s	0.2	0.56	2	3.5

Table 2: Decryption Time Of Symmetric Algorithms

	51 kB	**204 kB**	**407 Kb**	**1531 kB**
AES, s	3	5	7.6	8.23
DES, s	2	4.5	6	7.6
blowfish, s	1	2.3	3.5	5.6
RC6, s	100	134	233	435
IDEA, s	1.2	1.5	2.3	4.5

Table 3: Total Computation Time Of Symmetric Algorithms

	51 kB	**204 kB**	**407 Kb**	**1531 kB**
AES, s	8.7	10.6	15.6	20
DES, s	7	9	14	19
blowfish, s	5	7	8	11
RC6, s	200	232	345	678
IDEA, s	2	5	6	10

Table 4: Encryption Time

	51 kB	**204 kB**	**407 kB**	**1531 kB**	**3061 kB**	**6122 kB**	**9193 kB**
Paillier cryptosystem and digital signature, s	25	55	156	235	355	456	560
AES and MD5, s	1	2.5	3.7	9	12	19	24
CP-ABE and AES, s	3.5	4.5	6.5	13	15	24	30
blowfish and CP-ABE, s – SHS	1	1	2.5	8	9	15	20

Table 5: Decryption Time

	51 kB	**204 kB**	**407 Kb**	**1531 kB**	**3061 kB**	**6122 kB**	**9193 kB**
Paillier cryptosystem and digital signature, s	100	145	255	455	655	890	1000
AES and MD5, s	4.2	6	8.8	9	11	15	17.6
CP-ABE and AES, s	7.6	8.9	10.9	13.5	15	18	23
blowfish and CP-ABE, s – SHS	2.5	3.7	4.5	5.6	6.6	7.5	8.6

Table 6: Total Computation Time

	51 kB	**204 kB**	**407 kB**	**1531 Kb**	**3061 kB**	**6122 kB**	**9193 kB**
Paillier cryptosystem and digital signature, s	200	250	456	750	1100	1435	1600
AES and MD5, s	7	10	15	19	25	35	42
CP-ABE and AES, s	12	14	18	30	33	42	56
blowfish and CP-ABE, s – SHS	5	5.5	7.6	13	15.2	24	30

References

[1]. Castano F.J.G., Alonso J.V., Matencio P.L., et al.: Sensors, 2010, 10, pp. "Ambient intelligence systems for personalized sport training." 2359–2385

[2]. Lee H.J., Kumar P.: " Security concerns in wireless medical sensor network applications: a study, Sensors, 2012, 12, (1), pages 55–91,

[3]. Peng D., Wang W., and others: Body sensor networks for resource-aware, secure ECG healthcare monitoring, IEEE Wirel. Commun., 2010, 17, (1), pp. 12–19

[4]. Ersoy C., Alemdar H.: Healthcare wireless sensor networks: a poll, Computing Netw., 2010, 54, pp. 2688–2710

[5]. He D., S. Chan, and S. Tang: IEEE J. Biomed, "A novel and light-weight system for protecting wireless medical sensor networks." Health Care, 2014, 18, (1), pp. 23–32

[6]. Yi X, A. Bouguettaya, D. Georgakopoulos, and others: Medical sensor data privacy protection, IEEE Trans. Reliable Security Comput., 2015, 13, (3), pp. 369–380

[7]. Poon C.C.Y., Bao S.-D., Zhang Y.-T., and others: IEEE Trans., "Securizing a body sensor network by using the timing information of heartbeats as an identifier of an entity," Inf. Technol. Biomed., 2008, 12, (6), pp. 772–779

[8]. Khalil I, Ibaida A: IEEE Trans., "Wavelet-based ECG steganography for safeguarding patient private information in point-of-care systems." Biomed. Eng., 2013, 60, (12), pp. 3322–3330

[9]. Huang Y.M., M.Y. Hsieh, H.C. Chao, and others: IEEE J. Sel., "Pervasive, safe access to a sensor-based, hierarchical healthcare monitoring architecture in wireless heterogeneous networks." Common Domains, 2009, 27, (4), pp. 400–411

[10]. Cheng H., Hu C., Li H., et al.: IEEE Trans., "Safe and effective data communication protocol for wireless body area networks." Multiscale computation. Syst., 2015, 11, (14), pp. 1–11

[11]. Aggarwal K., Saini J.K., Verma H.K.: ' Evaluation of the RC6, blowfish, DES, IDEA, and CAST-128 block ciphers', International Comput. J. Appl., 2013, 68, (25), pp. 10–16

[12]. Abraham J., Masram R., Shahare V., and others: Analysis and comparison of various file features-based symmetric key cryptographic algorithms, International J. Netw. Secur. Appl. (IJNSA), 2014, vol. 6, p. 43–52

[13]. Levine M.M., Wasserman S.S., and Mackowiak P.A.: A critical evaluation of the upper limit of normal body temperature, 98.6°F, as well as other works of Carl Reinhold August Wunderlich, J. Am. Med. Assoc., 1992, 268, (12), pp. 1578–1580

[14]. Davis S., Liang S., Qiao Z., and others: IEEE Explore, "Survey of Attribute-Based Encryption," 2014, 00, pages 1–6,

[15]. S. Hohenberger, B. Waters: Quality based encryption with quick unscrambling'. Pages from Public-Key Cryptography: PKC (2013) (LNCS 7778) 162–179