Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.028089
Article

Tech Science Press

Authentication of WSN for Secured Medical Data Transmission Using Diffie Hellman Algorithm

A. Jenice Prabhu[1,*] and D. Hevin Rajesh[2]

[1]Arunachala College of Engineering for Women, Manavilai, Nagercoil, 629203, India
[2]St. Xavier's Catholic College of Engineering, Nagercoil, 629003, India
*Corresponding Author: A. Jenice Prabhu. Email: jeniceprabhu@gmail.com
Received: 02 February 2022; Accepted: 08 June 2022

Abstract: The applications of wireless sensor network (WSN) exhibits a significant rise in recent days since it is enveloped with various advantageous benefits. In the medical field, the emergence of WSN has created marvelous changes in monitoring the health conditions of the patients and so it is attracted by doctors and physicians. WSN assists in providing health care services without any delay and so it plays predominant role in saving the life of human. The data of different persons, time, places and networks have been linked with certain devices, which are collectively known as Internet of Things (IOT); it is regarded as the essential requirement of people in recent days. In the health care monitoring system, IOT plays a magnificent role, which has produced the real time monitoring of patient's condition. However the medical data transmission is accomplished quickly with high security by the routing and key management. When the data from the digital record system (cloud) is accessed by the patients or doctors, the medical data is transferred quickly through WSN by performing routing. The Probabilistic Neural Network (PNN) is utilized, which authenticates the shortest path to reach the destination and its performance is identified by comparing it with the Dynamic Source Routing (DSR) protocol and Energy aware and Stable Routing (ESR) protocol. While performing routing, the secured transmission is achieved by key management, for which the Diffie Hellman key exchange is utilized, which performs encryption and decryption to secure the medical data. This enables the quick and secured transmission of data from source to destination with improved throughput and delivery ratio.

Keywords: Probabilistic neural network (PNN); diffie hellman key exchange; internet of things (IOT); wireless sensor network (WSN)

1 Introduction

The emergence of WSN in healthcare sectors has produced multiple beneficial factors and so it is largely used in various fields. Some of the healthcare systems based on the WSN are electrocardiogram (ECG), blood pressure (BP), blood glucose (BG), in which the physiological data of patients are transmitted in real time [1]. The health care systems with WSN provide innovations thereby offering potential solutions and ambient awareness to the health care industry [2]. WSN comprises of various sensors with the properties like low cost, random deployment and self-organizing [3]. The data collected by the sensors are revealed on request without exposing the identity of sensors [4]. In WSN, the effective and efficient collection of data is achieved for all sensor nodes even if they are located in remote areas [5]. In harsh environments, the rapid delivery of data collected by sensors is facilitated by various encoding approaches [6]. Various devices are used for collecting the medical data, but they are excessively expensive for home utilization [7]. In recent times, the health monitoring has shown an intelligent trend due to the rapid development of IOT [8]. The IOT devices are neither practical nor scalable for relying on a central entity like cloud for performing the detection of misbehavior [9].

To overcome these issues, suitable routing techniques are utilized, through which the data availability is maximized and the data access latency is reduced [10]. The effective routing is performed by minimizing the number of transmissions, by which the life span of the system is accomplished. To enhance the energy efficiency and to find the appropriate routes, several researches have been developed. In [11], a clustering based routing approach is proposed for the collection of medical data in healthcare environment that relies on node centrality, distance and remaining energy level. It offers efficient energy clustering and forwards the data to the destination directly but requires further improvement related to network lifetime. In [12] an energy optimization algorithm is proposed to provide appropriate communication with optimized routing paths. This approach improves the data transmission speed and power efficiency yet did not consider the security related issues. In [13] an enhanced routing approach for mobile cognitive environments is introduced by considering the cross-layer design and mobility design. Under larger network area, flooding packets get limited due to sparse node density which in turn reduces routing packets. To enhance the system efficiency, motion based routing is utilized in [14], which computes the system utility by storing and using the local motion information, where the system lifespan depends on the movement of the neighboring node. To overcome these issues neural networks are adopted for the prediction of efficient routing in IOT based WSN. In [15], the routing approach in WSN based on Artificial Neural Networks (ANN) is explained which analyses the best path for routing. ANN has the ability to learn complex and non-linear relationships but highly depends on hardware. Considering these shortcomings, PNN is utilized in this developed paper for the prediction of efficient routing path.

Generally, the privacy of medical data is highly important for personal privacy information and hence the related security is essential [16]. The confidential data of medical sectors have been transmitted through the internet for multiple purposes, in which the security of particular data is lacking since the medium of transformation is not secured enough [17]. The privacy and security of medical data face various challenges like transmission reliability, integrity, location privacy and data confidentiality [18]. Unauthorized access to sensitive medical data occurs which include hijacking of medical devices, health data modification, exploitation of stored and exchanged information, gaining access to hospital networks [19]. By using key management approaches, the data is secured between the implanted medical device and cloud server but the performance is not scalable. The issues in the key management are identified by the certificate-based pairing free aggregate signature scheme (CBPFAS), which accomplishes public key cryptography along with its identity. However, the mentioned approach requires reduction of aggregation length [20]. For better result, light weight mutual authentication and key aggregation (MAKA) is utilized as it acts against the potential attacks and contemporary authentication but it performs with little delay [21]. In [22], for the yield of secure channel, the Elliptic Curve Cryptography (ECC) based self-certified two factor key management is utilized, which suffers from cluster and head impersonation. In medical data communication, the acquired error is identified as diffusion and confusion; the investigation is enhanced by medical image with a couple of sub-keys [23], in which the keys are not performed heavily. In [24], a method for coverless information hiding is proposed using the Generative Adversarial Networks (GAN) based key management. It provides enhanced hidden capacity but lags in robustness and demands optimization process. In [25], the proposed approach for coverless information hiding retains the data without any changes yet, the time cost is high. To overcome these issues, Diffie Hellman key is utilized in this work for effective key management.

Similar approaches for the secured key management of medical data are proposed in [26] and [27]. These approaches increase the security of medical data and maximizes the accuracy of medical data analysis but requires further improvement. In this paper, both the personal and health rate of the patients are stored in the digital record system (cloud), through which the patients and doctors can retrieve the medical details from cloud at any time and when the medical data is transmitted from digital record system (source node) to patients (destination node), the PNN routing protocol is used to transmit the data quickly. For the secure transmission, the Diffie Hellman keys are utilized, which encrypts and decrypts the data in a secured manner. In this developed paper, the proposed system model is given in the Section 2, the result and discussion of this proposed method is given in Section 3 and this developed paper is concluded in the Section 4.

2 Proposed System

The proposed method is developed to maximize the applicability of future networking methods and through this, certain applications are linked with each other to gather the information with the aid of internet. WSN is immensely beneficial in the health care sectors because it provides extreme assistance to both the patients and the doctors for enhancing the health condition of the patients. To enhance the human health, the health monitoring systems with various sensors are developed. The human health conditions thus monitored are further stored in the cloud. From the cloud the doctors or patients can access their data at any time and any situation. For the better communication, IOT is utilized which interacts through the internet, the informations thus generated is computed by clouds. The medical data from cloud to the patients are transmitted quickly by performing PNN based routing. While performing routing, the safest transmission is achieved by Diffie Hellman key management technique.

2.1 Proposed Patient Monitoring System

In recent days, the health care centers are increased into multiple levels, which are located in different locations and each center provides a large amount of crucial health data. This health related data are stared, with an aim that doctors can examine the diseases and also the medical history of patients are studied. The overtime monitoring of health is achieved by deploying several IOT devices and the transfer of high volume medical data at real time is laborious. In general, the high level, medical data are qualified by the clouds rapidly but for real-time, it is difficult to gain the large volume of data from all IOT devices due to the presence of bandwidth limitation and cloud distance. These result in process delay and to eliminate these issues cloudlet is utilized to store medical data which transmits the medical data to the nearest IOT device. The burden in the communication is achieved by cloudlet and then the data is transferred to the cloud. Thus the transmission of medical data is achieved by two layers like, IOT layer, and cloud layer.

The Patient monitoring system is significantly highlighted in Fig. 1 in an efficient manner.

2.1.1 IOT Layer

The patient monitoring system is achieved by IOT frame work which alerts the patient about the occurrence of abnormal signs. The IOT monitoring of the patient is achieved by four major dimensions such as sensing, analyzing, managing and deleting, which are clearly illustrated in Fig. 2.

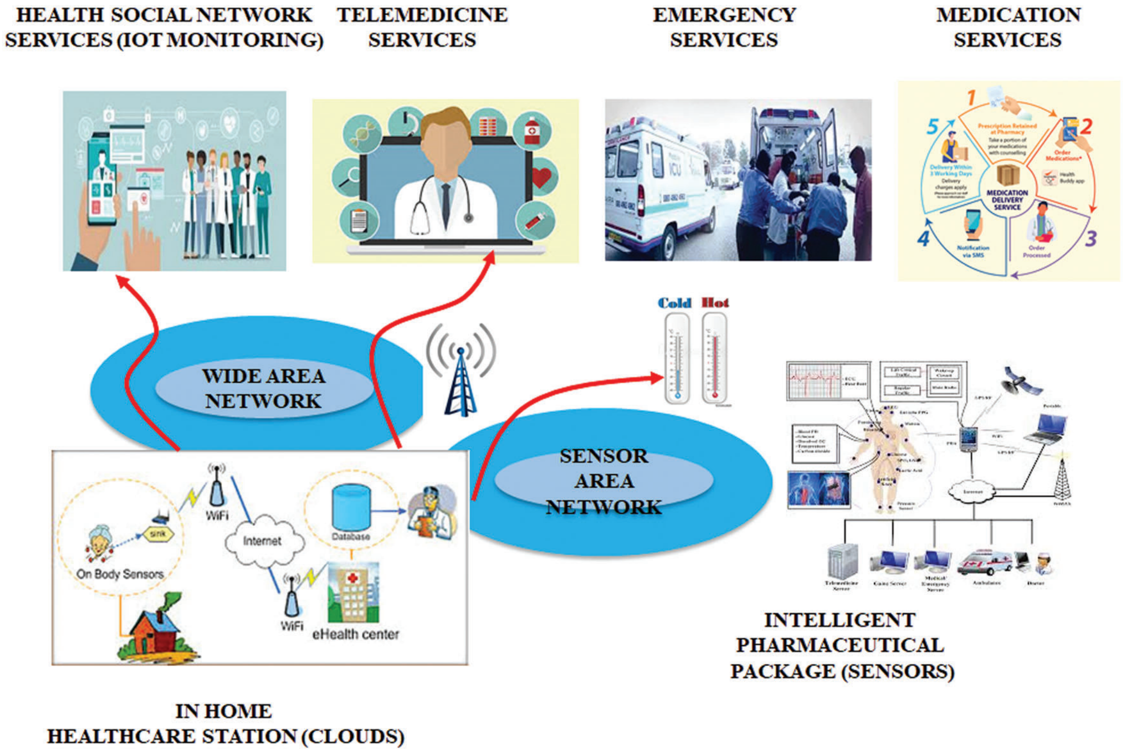

Figure 1: Patient monitoring

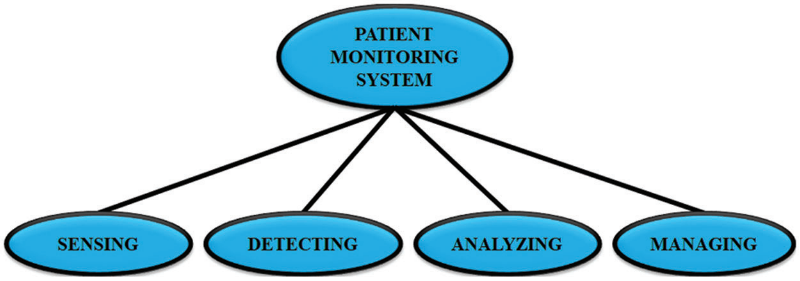

Figure 2: Dimensions of IOT layer

The sensors in IOT monitoring sense the accurate location and gather the information, this collected abnormalities do not project any defect. The change in weather may cause abnormal behaviors but usually the area damage is identified by the abnormal behavior. The defects in the data are analyzed by sensing the data delivered from the sensor nodes. From the analyzed data, the prediction of issues in particular area is achieved by management. This compares the present data with the past history, so that the issues are detected accurately and then the patients are alerted. The gained data are then stored in the cloud and by cloud computing data are utilized by the patients through the device like mobile phones.

2.1.2 Cloud Layer

The storing of data in the cloud is mentioned as the cloud computing and it runs the operation connected to it. The general value of the regular data is continued by the transmitted regular data which accommodate the actual function in the great extent. Thus the general functions are maintained by the quality service.

Cluster computing is performed by storing the data in the cloud through which the applications are functioning. With the aid of internet, the data which are stored in cloud has been linked with multiple computers. The people from different locations can access the data from cloud and one of the major advantage in cloud computing is that the data in cloud are stored securely even if it is crashed. The patient details regarding their contact and treatment are stored in the cloud and the information from cloud is displayed through IOT.

2.2 Routing Protocol

The significance of routing protocol in the process of data transmission is highly essential since the communication between the nodes is determined through this protocol. Though the routing protocol has easy implementation, it has certain challenges, which are mentioned in the sub-sequent point. The design of routing protocol in WSN is challenging due to the presence of the multiple characteristics, the important challenges of routing are

- For the large set of sensor nodes, the allocation of universal identifiers is difficult and the use of classical Internet Protocol (IP) makes the WSN un-proficient.
- The flow of data to be transmitted from a source node to the base station is compulsory and at typical communication network the transmission of data is not performed.
- In several circumstances the data congestion is created with substantial redundancies since the sensing of nodes generates similar data. Thus the exploitation of routing protocols is necessary and the required energy and bandwidth is utilized.
- For the relations of transmission energy, bandwidth, capacity and storage the WSN is constrained. To overcome these challenges the new routing protocols are implemented, which eliminates these routing challenges.

Authentication of PNN Routing Protocol

The medical data stored in the clouds are accessed by the patients through IOT and the data is transferred by identifying the shortest path, which is performed by routing probabilistic Neural Network (PNN). The regulation of data transfer became critical, when the number of nodes are increased and the nodes with dominated sets (DS) contain increased connectivity and energy, this is classified by PNN and the node scalability is achieved by the clusters. In PNN the transferred data is trained by the hidden layer in which the sensor nodes are replaced with the clusters, by this the data from each node is trained separately.

At each node, the hidden layer function is denoted as,

$$H_{ij} = \exp\left[\frac{\sum_{ij\varepsilon}^{\mu} .c_{\varepsilon} - 1}{\sigma_{ij}}\right] \tag{1}$$

Here, $\mu_{ij\varepsilon}$ denotes cluster weight vector, σ_{ij} denotes cluster standard deviation and c_{ε} denotes cluster energy. While performing routing the nodes are exhibited by node dynamics and the interconnections of node are performed with other networks. In Neural Network the former and later sensor nodes are considered as the input, here PNN is the utilized Neural Network which enhances and classifies the lifespan of Network through DS. The architecture of PNN is efficiently highlighted in Fig. 3.

The identification of route is important for the communication of data and consumption of energy during routing performance; through the identified route the cluster is formed and the lifespan is improved. Each sensor node divides the clusters $c_1, \ c_2 \ldots, \ c_n$ which are needed as the PNN input. The selection of trained data is achieved by PNN, which selects higher energy data as trained data i.e., cluster. The cluster k as trained data is permitted in WSN by n number of sensor nodes i.e., $x_i, \ i = 1 \ldots n$, after cluster is allotted for each sensor nodes (shortest distance) and the threshold for each distance is measured.

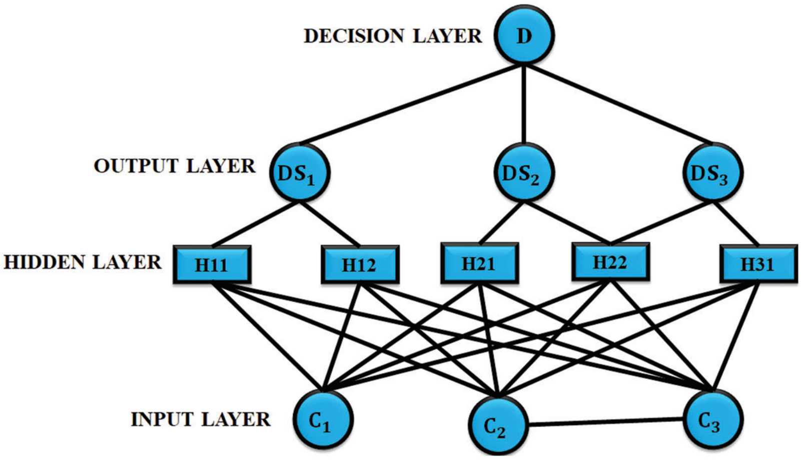

Figure 3: PNN structure

The routing is performed to transmit the data quickly, here PNN performs the routing function.

The formation of cluster in PNN is achieved by the given procedure,

Step 1: Initially the cluster center is obtained as $\mu_i = T,\ \ i = 1\ldots,\ k.$

Step 2: Nearest node of the cluster is analyzed

$$c_i = \{i = d(x_j,\ \mu_i \leq dx_j,\ \mu_i),\ l \neq i,),\ j = 1\ldots j$$

Step 3: From the mean distance node, the cluster locations are identified.

$$\mu_i = 1|c_i| \sum^{j} \in c_i x_j,\ \forall_i$$

Step 4: Repeat step 2 and 3, until the cluster is designed,

In which, the sensor node in c is signified as $|c|$, nearby node of c is c_i,

The cluster utilize the Euclidean distance d(x, μ_i) as,

$$c_k = d(x_1,\ y_1),\ \ d(x_2,\ y_2)\ldots d(x_i,\ y_i),\ \ i = 1,\ \ldots,\ n,\ \ j = 1,\ \ldots,\ n.$$

Here, k denotes the cluster node Algorithm for cluster formation

The medical data stored in the cloud are transmitted by utilizing the PNN, which authenticate the shortest path for transmission and reach the destination (patient IOT page) quickly. The data transmission is secured with the accomplishment of keys.

2.3 Key Management

For the secured communication of medical data, key management functions are utilized and in this work Diffie Hellman key is used. By this the functions like authentication, authorization, encryption and decryption are performed.

Authentication of Diffie Hellman Key

The cryptographic keys are distributed using an instant key, that is Diffie Hellman key which responses instantly. For undetermined channels, the secret keys are developed by Diffie Hellman keys in the lack of premature learning that authorize two gatherings. This key performs their functions by i) develop new registration for cloud service, ii) cloud service utilization, iii) key exchange.

2.3.1 Develop New Registration for Cloud Service

Initially the patients or organizations are selected and established on the basis of cloud administration. Among different understatement of patients i.e., patient id, email and portable number, the patient is approved by utilizing portable number, this identifies whether the client is authentic or not. The enlistment of clients is obtained by promoting the instant message that is given to the client and is recorded in the cloud. The secret key is produced when the client enters the client id and these generated keys are considerable in a particular interval or these keys are demolished after a particular interval.

2.3.2 Cloud Service Utilization

Among the enlisted patients, the patient with cloud administrations are selected by the cloud. The patients are allowed to enter their id and secret phrase, on verification, the Diffie Hellman key exchange algorithm generates the new key and it is forwarded to the patients through phone, email, etc. The entry point for the patient is obtained in their apparatus, after this the generated keys are given to the cloud administrations.

2.3.3 Key Exchange

The Diffie Hellman key exchange setup a common key between the two gatherings, which compensate the information, correlation along the framework. This key exchange does not require extensive number of characters. It is difficult to break the security, when the cryptographic system utilize secret key all through the encryption and decryption, the Diffie Hellman key exchange is achieved by the following algorithm.

Algorithm for Diffie-Hellman key exchange

Step 1: The secret key between the doctor and patient is identified by using Diffie Hellman key as $A^{pd} = B \in M$,

Where A^{pd} is a computed data from both the doctors and patients

Step 2: The map of B is given to the group G by patients and doctors then the data is received as $B_g \in G$.

Where G refers to the group of medical information

Step 3: By multiplying M and B_g, the message ($M \in G$) is encrypted as

$M * B_g = Y$ and the encrypted message Y is transmitted to the patients.

Step 4: The patients decrypts the message by computing B_g inversely and receive the message M as,

$Y * B_g^{-1} = M$

Where, M is a decrypted message.

Evaluation of Diffie-Hellman Key Exchange:

Initially, the matrix A is considered which is referred as an initial data $A = \begin{pmatrix} 6 & 2 & 1 \\ 3 & 4 & 9 \\ 9 & 0 & 7 \end{pmatrix}$

Patient send the secret code as, $A^p = A^6 = \begin{pmatrix} 9 & 8 & 6 \\ 4 & 8 & 5 \\ 0 & 6 & 7 \end{pmatrix}$

Doctor send the secret code as, $A^d = A^9 = \begin{pmatrix} 3 & 4 & 6 \\ 0 & 8 & 1 \\ 6 & 2 & 3 \end{pmatrix}$

Thus the shared key is, $\text{x}A^{pd} = A^{54} = \begin{pmatrix} 7 & 8 & 8 \\ 6 & 8 & 9 \\ 4 & 2 & 9 \end{pmatrix} = B$

Initially, the patient consider the message as $M = (6,\ 7,\ 10,\ 4,\ 1,\ 5,\ 5,\ 2,\ 9) \in G$

The map of B is achieved by adding a unit term with each matrix elements, thus the patient sends the data as $\begin{pmatrix} 7 & 8 & 8 \\ 6 & 8 & 9 \\ 4 & 2 & 9 \end{pmatrix} = B$ and the mapped value of B into group is,

$B_g = (8,\ 9,\ 9,\ 7,\ 9,\ 10,\ 5,\ 3,\ 10)$

The group G as $(g_1,\ g_2,\ \ldots,\ g_g)|g_i \in Z_{11}^*$ is multiplied with the components $(x_1,\ x_2,\ \ldots,\ x_g)$ as $(x_1,\ x_2,\ \ldots,\ x_g) * (g_1,\ g_2,\ \ldots,\ g_g) = (x_1 * g_1,\ x_2 * g_2,\ \ldots,\ x_g * g_g)$

The message M is multiplied with B_g through mod 11

$$(6,\ 7,\ 10,\ 4,\ 1,\ 5,\ 5,\ 2,\ 9) * (8,\ 9,\ 9,\ 7,\ 9,\ 10,\ 5,\ 3,\ 10)$$

$$= (6 * 8,\ 7 * 9,\ 10 * 9,\ 4 * 7,\ 1 * 9,\ 5 * 10,\ 5 * 5,\ 2 * 3,\ 9 * 10) \quad mod\ 11$$

$$= (4,\ 8,\ 2,\ 6,\ 9,\ 6,\ 3,\ 6,\ 2)$$

The encrypted message that send by the patient to doctor is

$Y = (4,\ 8,\ 2,\ 6,\ 9,\ 6,\ 3,\ 6,\ 2)$

Doctor takes $\begin{pmatrix} 7 & 8 & 8 \\ 6 & 8 & 9 \\ 4 & 2 & 9 \end{pmatrix} = B$, and it is mapped as $(8,\ 9,\ 9,\ 7,\ 9,\ 10,\ 5,\ 3,\ 10)$ then the inverse computation is performed in B_g modulo 11, and requires

$$(8,\ 9,\ 9,\ 7,\ 9,\ 10,\ 5,\ 3,\ 10)^{-1} = (7,\ 5,\ 5,\ 8,\ 5,\ 10,\ 9,\ 4,\ 10)$$

Thus the original is obtained by multiplying encrypted message with the inversed value,

$$(4,\ 8,\ 2,\ 6,\ 9,\ 6,\ 3,\ 6,\ 2) * (7,\ 5,\ 5,\ 8,\ 5,\ 10,\ 9,\ 4,\ 10) \quad mod\ 11$$

$$= (4 * 7,\ 8 * 5,\ 2 * 5,\ 6 * 8,\ 9 * 5,\ 6 * 10,\ 3 * 9,\ 6 * 4,\ 2 * 10)$$

$$= (6,\ 7,\ 10,\ 4,\ 1,\ 5,\ 5,\ 2,\ 9)$$

This is the original message M that is encrypted by the patient to the doctor. By these functions, the medical data from the cloud are transmitted to the clients or doctors securely with the secret key generation by Diffie Hellman algorithm.

3 Results and Discussions

The IOT is a huge network, which includes the objects or devices that perform communication via wireless and cable connections, also the IOT interacts with each one to develop new services. The IOT is one of the most popular technique which is used in the medical field, by this the human conditions (temperature, pressure, and pulse) are monitored continuously. The IOT monitoring of patient conditions are shown in the Fig. 4. The overtime monitoring of patients health is achieved by developing several

IOT devices and the transfer of high volume medical data at real time is laborious. In general the medical data and personal information of the patients are stored in the cloud, which can be accessed by both the patients and doctors. The monitored medical data like body temperature, blood pressure and pulse, etc., are gathered in the cloud. The access of the stored data by patients or doctors from the cloud faces severe security issues, to overcome this issue fast transmission is performed. For the quick transmission of medical data, routing is performed and the transmission of data is secured by key management. The data from the sensor node to the IOT page is transmitted by passing the data through wireless sensor network.

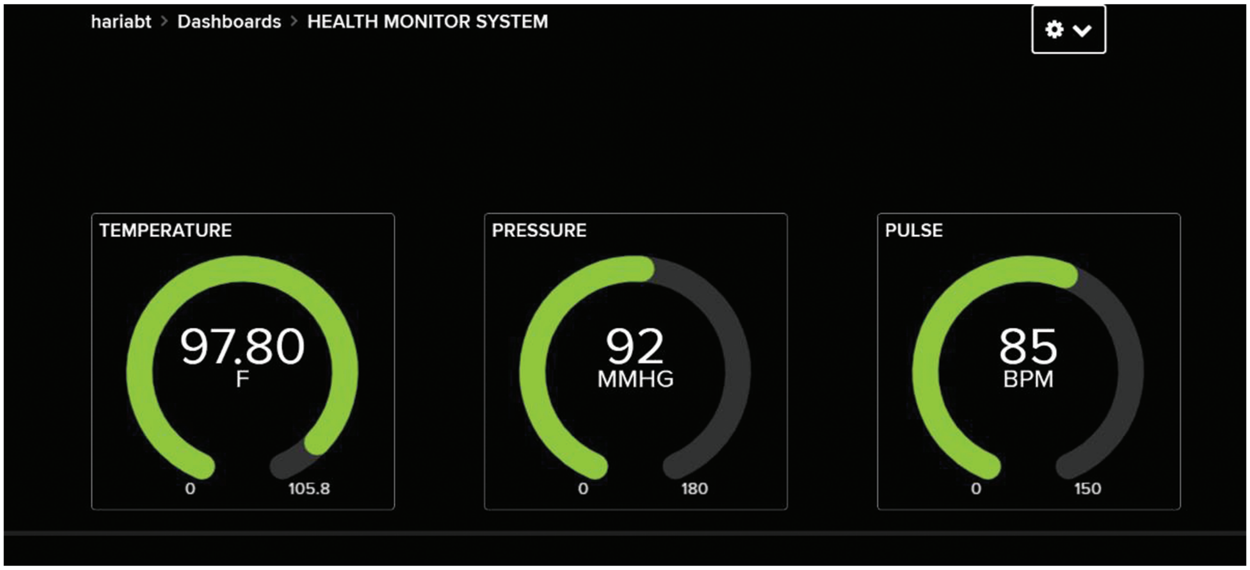

Figure 4: IOT monitoring

The transfer of medical data is achieved quickly by routing, by this the shortest path to the destination is identified and then the data is transmitted. In this developed paper, PNN is utilized to perform routing and its performance is identified by comparing it with the existing DSR and ESR. Here the communication rank is varied as 100, 200, 300, 400, 500 m in which the delivery ratio, delay, energy consumption, throughput and packet drop of PNN is identified by the transmission range.

From the Fig. 5, the delivery ratio of the proposed PNN is compared with the existing methods DSR and ESR, which concludes that the PNN shows better result that other two methods.

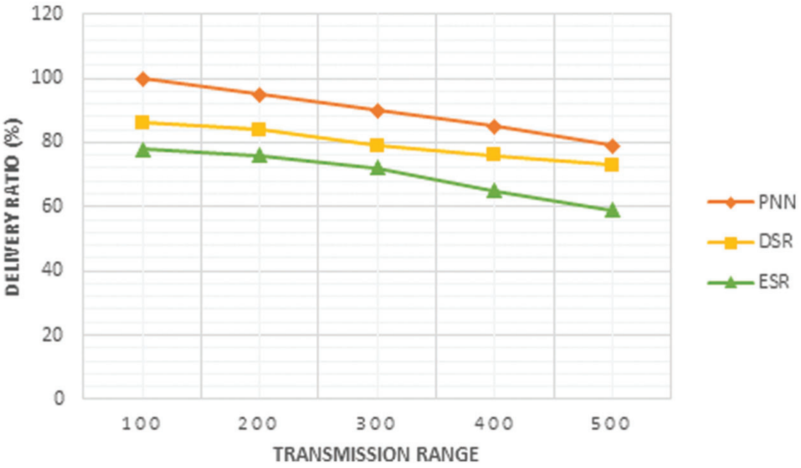

Figure 5: Plot of transmission range and delivery ratio

The delay estimation for the proposed PNN is obtained by comparing it with the existing DSR and ESR, which is shown in the Fig. 6 from this it is clear that the delay in PNN is less than other existing methods.

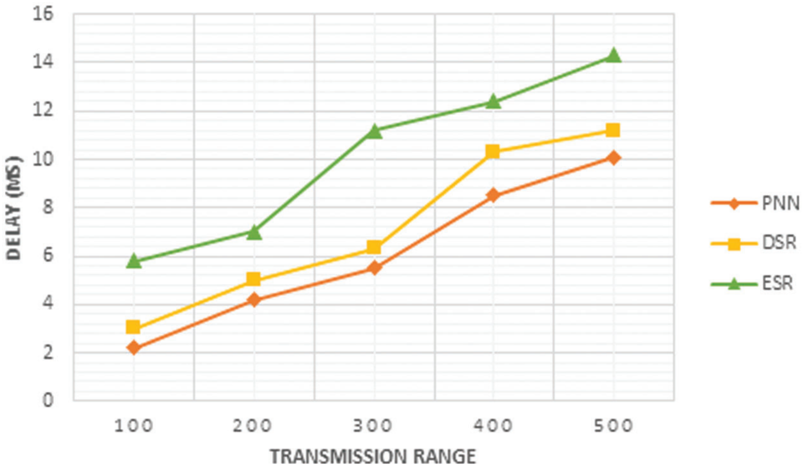

Figure 6: Plot of transmission range and delay

The estimation of energy consumption by PNN is obtained by comparing it with the existing DSR and ESR, which is shown in the Fig. 7 from this it is concluded that the energy consumed by the PNN is less than other existing methods.

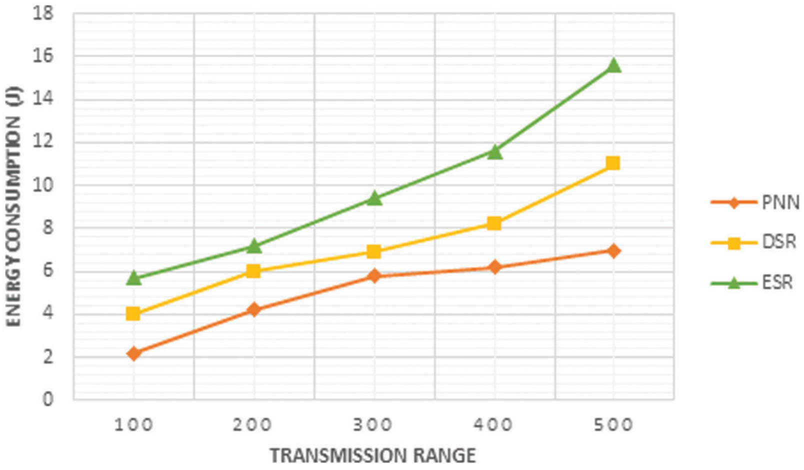

Figure 7: Plot of transmission range and energy consumption

The throughput of PNN is evaluated by comparing it with the existing DSR and ESR methods which is shown in the Fig. 8, this figure concludes that the throughput of the proposed PNN is higher than the other existing methods.

From the Fig. 9, the packet drop of the PNN is compared with the existing DSR and ESR methods, which concludes that the drop in PNN is lower than other methods.

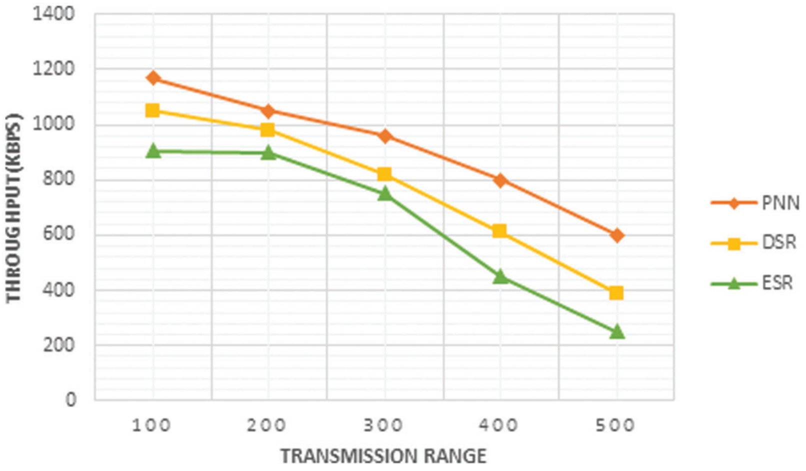

Figure 8: Plot of transmission range and throughput

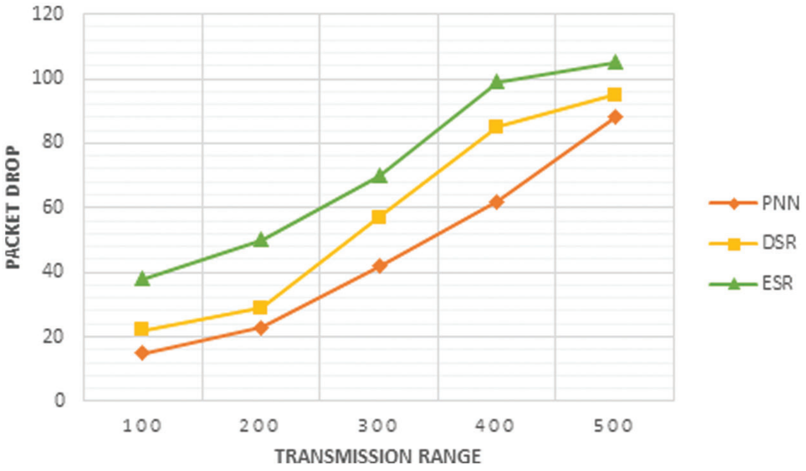

Figure 9: Plot of transmission range and packet drop

Evaluation of Encryption and Decryption Performance

Generally, the keys are utilized to transmit the data securely and safely, which performs both the encryption and decryption. Each key is created in a specific interval of time and the time required for the key generation is shown in the Fig. 10. The medical data stored in the cloud are accessed by both the patients and doctors during which the keys generated within a short time. However, the key encryption and decryption is also performed with the required time interval.

As per the data size, the key encryption and decryption is performed and the size of the data is increased further increasing the time required for encryption and decryption. When the data stored in the cloud is accessed, the key encryption is initiated and after reaching the destination the encrypted data is decrypted with the required interval of time.

From the Figs. 11 and 12, it is clear that the size of the data is increased leading to increased time interval. However, the time required for the key generation, key encryption and decryption is less for the proposed Diffie Hellman Key exchange.

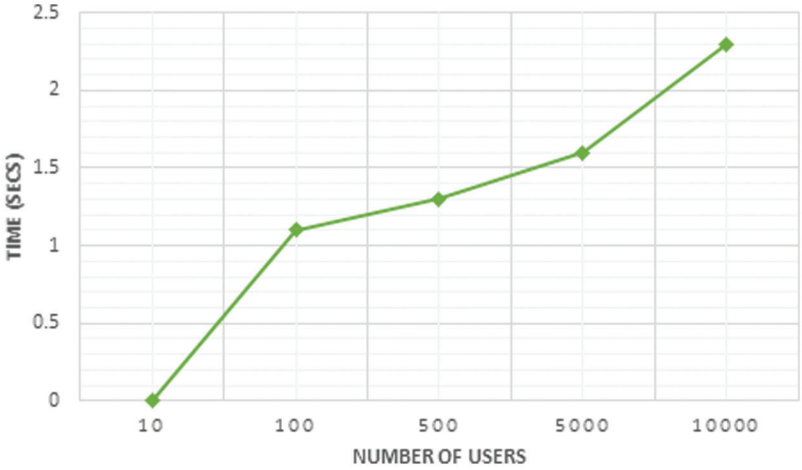

Figure 10: Essential time for key generation

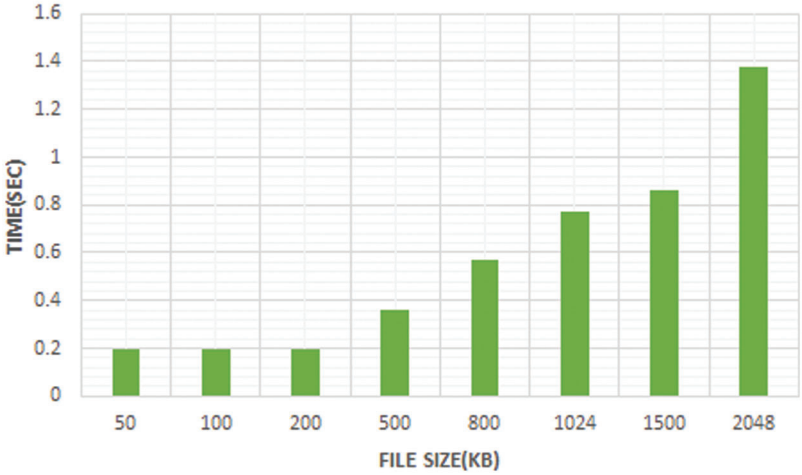

Figure 11: Essential time for encryption

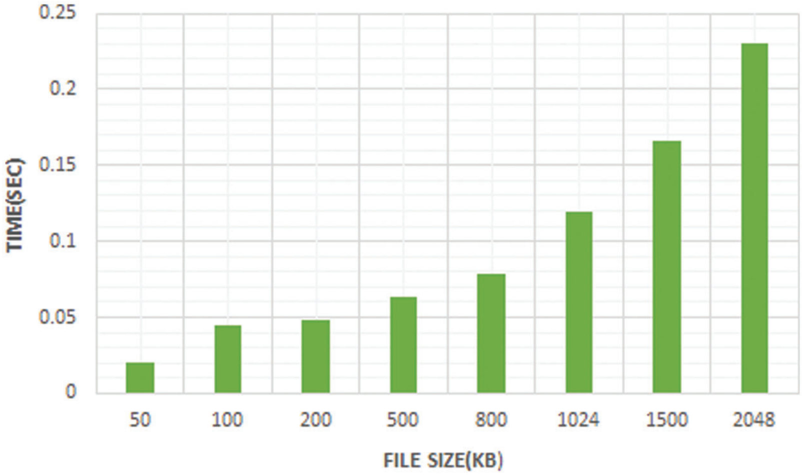

Figure 12: Essential time for decryption

Thus the medical data from the cloud are accessed safely and quickly by routing and key management. Here the routing is performed by the PNN which identifies the shortest path to reach its destination and the performance of the PNN related to delivery ratio, delay, throughput and packet drop are identified by comparing it with the existing DSR and ESR methods. While performing routing the medical data is secured by key management, here the Diffie Hellman key exchange is utilized which performs the encryption and decryption as per the data size. Thus the medical data from the clouds are transmitted quickly and securely to the users who access it.

4 Conclusion

The protection of medical data with Diffie Hellman key is expounded in this present work, in which the implementation of PNN is clearly explained. Initially, the medical data stored in the cloud is transmitted to the user through WSN and the resultant data are viewed in the IOT page. The transmission of medical data from the cloud is transmitted quickly and securely by routing and key management. In this developed paper, the routing is performed by PNN and its performance is accomplished by comparing it with the DSR and ESR. For the secured transmission, Diffie Hellman key is utilized, which performs both the encryption and decryption. The obtained results reveal the efficiency of the proposed approach in terms of routing and key management.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Lee and W. Chung, “A robust wearable u-healthcare platform in wireless sensor network,” *Journal of Communications and Networks*, vol. 16, no. 4, pp. 465–474, 2014.

[2] A. Alaiad and L. Zhou, “Patients’ adoption of WSN-based smart home healthcare systems: An integrated model of facilitators and barriers,” *IEEE Transactions on Professional Communication*, vol. 60, no. 1, pp. 4–23, 2017.

[3] R. Kocherla, M. Chandra Sekhar and R. Vatambeti, “Enhancing the energy efficiency for prolonging the network life time in multi-conditional multi-sensor based wireless sensor network,” *Journal of Control and Decision*, pp. 1–10, 2022. http://dx.doi.org/10.1080/23307706.2022.2057362.

[4] T. Chatterjee, S. Karmakar and S. Das Bit, “IPLQueeN: Integrity preserving low-overhead query handling over NDN-based WSN,” *IEEE Access*, vol. 9, pp. 82786–82811, 2021.

[5] X. Wang, X. Liu, C. -T. Cheng, L. Deng, X. Chen *et al.,* “A joint user scheduling and trajectory planning data collection strategy for the UAV-assisted WSN,” *IEEE Communications Letters*, vol. 25, no. 7, pp. 2333–2337, 2021.

[6] C. Han, J. Yin, L. Ye, Y. Ke and Y. Yang, “An integrated fast data transmission scheme based on network coding,” *IEEE Access*, vol. 7, pp. 112216–112228, 2019.

[7] G. Xu, “IOT-Assisted ecg monitoring framework with secure data transmission for health care applications,” *IEEE Access*, vol. 8, pp. 74586–74594, 2020.

[8] H. Zhang, J. Li, B. Wen, Y. Xun and J. Liu, “Connecting intelligent things in smart hospitals using NB-IOT,” *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1550–1560, 2018.

[9] G. Choudhary, P. V. Astillo, I. You, K. Yim, I. Chen *et al.,* “Lightweight misbehavior detection management of embedded iot devices in medical cyber physical systems,” *IEEE Transactions on Network and Service Management*, vol. 17, no. 4, pp. 2496–2510, 2020.

[10] T. M. Godinho, C. Viana-Ferreira, L. A. B. Silva and C. Costa, “A routing mechanism for cloud outsourcing of medical imaging repositories,” *IEEE Journal of Biomedical and Health Informatics*, vol. 20, no. 1, pp. 367–375, 2016.

[11] G. Kadiravan, P. Sujatha, T. Asvany, R. Punithavathi, M. Elhoseny *et al.,* “Metaheuristic clustering protocol for healthcare data collection in mobile wireless multimedia sensor networks,” *Computers, Materials & Continua*, vol. 66, no. 3, pp. 3215–3231, 2021.

[12] S. K. Swmi Durai, B. Duraisamy and J. T. Thirukrishna, “Certain investigation on healthcare monitoring for enhancing data transmission in WSN,” *International Journal of Wireless Information Networks*, pp. 1–8, 2021. http://dx.doi.org/10.1007/s10776-021-00530-x.

[13] F. Tang, M. Guo, S. Guo and C. Xu, “Mobility prediction based joint stable routing and channel assignment for mobile ad hoc cognitive networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 3, pp. 789–802, 2016.

[14] G. Newell and G. Vejarano, “Motion-based routing and transmission power control in wireless body area networks,” *IEEE Open Journal of the Communications Society*, vol. 1, pp. 444–461, 2020.

[15] Q. Ding, R. Zhu, H. Liu and M. Ma, “An overview of machine learning-based energy-efficient routing algorithms in wireless sensor networks,” *Electronics*, vol. 10, no. 13, pp. 1539, 2021.

[16] K. Fan, W. Jiang, H. Li and Y. Yang, “Lightweight RFID protocol for medical privacy protection in IOT,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1656–1665, 2018.

[17] S. Kumari, P. Chaudhary, C. Chen and M. K. Khan, “Questioning key compromise attack on ostad-sharif *et al.*’s authentication and session key generation scheme for healthcare applications,” *IEEE Access*, vol. 7, pp. 39717–39720, 2019.

[18] C. H. Tseng, S. Wang and W. Tsaur, “Hierarchical and dynamic elliptic curve cryptosystem based self-certified public key scheme for medical data protection,” *IEEE Transactions on Reliability*, vol. 64, no. 3, pp. 1078–1085, 2015.

[19] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. P. C. Rodrigues *et al.,* “BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment,” *IEEE Access*, vol. 8, pp. 95956–95977, 2020.

[20] G. K. Verma, B. B. Singh, N. Kumar, O. Kaiwartya and M. S. Obaidat, “PFCBAS: Pairing free and provable certificate-based aggregate signature scheme for the e-healthcare monitoring system,” *IEEE Systems Journal*, vol. 14, no. 2, pp. 1704–1715, 2020.

[21] K. Park, S. Noh, H. Lee, A. K. Das, M. Kim *et al.,* “LAKS-NVT: Provably secure and lightweight authentication and key agreement scheme without verification table in medical internet of things,” *IEEE Access*, vol. 8, pp. 119387–119404, 2020.

[22] D. Abbasinezhad-Mood and M. Nikooghadam, “Efficient design of a novel ECC-based public key scheme for medical data protection by utilization of nanoPi fire,” *IEEE Transactions on Reliability*, vol. 67, no. 3, pp. 1328–1339, 2018.

[23] K. Shankar, M. Elhoseny, E. D. Chelvi, S. K. Lakshmanaprabu and W. Wu, “An efficient optimal key based chaos function for medical image security,” *IEEE Access*, vol. 6, pp. 77145–77154, 2018.

[24] Y. Cao, Z. Zhou, Q. M. Wu, C. Yuan and X. Sun, “Coverless information hiding based on the generation of anime characters,” *EURASIP Journal on Image and Video Processing*, vol. 2020, no. 1, pp. 1–15, 2020.

[25] Y. Tan, J. Qin, X. Xiang, C. Zhang and Z. Wang, “Coverless steganography based on motion analysis of video,” *Security and Communication Networks*, 2021. http://dx.doi.org/10.1155/2021/5554058.

[26] X. Cheng, F. Chen, D. Xie, H. Sun and C. Huang, “Design of a secure medical data sharing scheme based on blockchain,” *Journal of Medical Systems*, vol. 44, no. 2, pp. 1–11, 2020.

[27] A. Tolba and Z. Al-Makhadmeh, “Predictive data analysis approach for securing medical data in smart grid healthcare systems,” *Future Generation Computer Systems*, vol. 117, pp. 87–96, 2021.