International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Prioritized Compressed Data Acquisition Framework for Securing the Data Integrity in the Medical Wireless Sensor Networks

B. Naresh Kumar[1], M. Srinivas[2*]

Submitted: 06/02/2024 **Revised:** 14/03/2024 **Accepted:** 20/03/2024

Abstract: MWSNs are essential in enhancing healthcare systems by delivering efficient and effective solutions. These allow elderly and disabled individuals to live independently while ensuring their well-being and safety. In hospitals, the data collected by the sensors deployed in these networks can be analyzed in real time. To ensure the safety and confidentiality of the data collected by MWSNs, it is important that the information is properly aggregated and transmitted to the appropriate central servers. This process should be performed with the utmost security to avoid unauthorized access and manipulation of the data. This paper proposes a prioritized compressed data acquisition framework that is designed to increase the efficacy of gathering various health information types. The framework utilizes a sampling technique known as compressed sensing to reduce the transmission overhead and power consumption. Data is then encrypted, and its integrity is protected through a cryptographic hash protocol. The priority of the information is then considered, and the transmission is performed according to the usual method. The security aspects of the proposed framework are analyzed to ensure that the data collected by the MWSNs is protected. In addition, we performed an experiment on the system's performance. The findings of the study indicate that the proposed system can help improve the quality of healthcare by allowing more accurate and timely information.

Keywords: *Data security, MWSNs, Compression, Encryption.*

1. Introduction

The development of new technologies such as wireless communications, information processing, and microelectronics has led to the creation of compact and energy-efficient sensor nodes. Using wireless communication [1], these sensor nodes can establish a wireless sensor network. These networks are being used for various applications such as home automation, industrial control, and healthcare [2]. Over the past decade, the use of wireless sensor network technology has been increasing in various health applications [3]. In this area, sensors are placed on the body to collect various biological signals, which can be controlled by the type of sensor that's used [4]. Through this technology, the readings can be analyzed by a medical professional, who can then take appropriate action to improve the patient's condition [5]. The goal of these wireless sensor systems is to improve the quality of life for older individuals and lower the costs of their healthcare. [6].

In some cases, patients require continuous monitoring and need to be kept in a hospital for a long time. [7]. Typically, a range of medical parameters need to be constantly recorded for such patients. For instance, in the case of an electrocardiogram (ECG), multiple sensors must be attached to the patient. However, utilizing wired connections to attach numerous sensors can cause significant discomfort. Alternatively, the use of medical wireless sensor network (MWSN) technology allows patients to experience freedom of movement. In addition, hospitals can equip themselves with MWSN nodes that allow patients to move around while still maintaining their connection to the network [8]. In today's context, data security has become a crucial necessity across a wide range of applications. Maintaining the security of medical information exchanged between sensing nodes (SNs) and healthcare centers is a significant concern for both healthcare professionals and patients [9, 10]. It is imperative to uphold the integrity and freshness of medical data to ensure accurate and prompt responses [6, 7]. MWSNs must be secure as they collect data related to a patient's condition.

There are many challenges that MWSNs face when it comes to developing an efficient and secure system. Firstly, there is a multitude of security requirements that must be met. Secondly, the security mechanisms employed need to be resource efficient. This is a challenging task due to the energy supply, processing speed, bandwidth, and memory limitations of sensor nodes, particularly those implanted. [11]. Due to the limited resources of sensor nodes, the implementation of cryptographic methods can be considered impractical or impossible in many scenarios [12].

2. Network Architecture

This scenario explores the use of a sensor-based system in a hospital setting. We will look into a deployment scenario wherein several sensors are placed on the body of a patient. The MWSN is built on the foundation of sensors that are placed on the body. These components are designed to continuously monitor the health conditions of patients. Medical sensor networks are composed of devices that are attached to a patient's body and can communicate with a variety of external devices to provide continuous health information. Through the use of sensors, patients can receive prompt responses to various health conditions. For instance, an implanted glucose sensor can continuously monitor the glucose levels of a patient. In addition, we introduce a new node in sickbeds that has more advanced capabilities than other body nodes. This new component has a

[1]*Research scholar, Department of CSE, koneru lakshmaiah Educational Foundation, Vaddeswaram, AP,India.*
ORCID ID : 0009-0008-0679-9403
[2]*Professor, Department of CSE, koneru lakshmaiah Educational Foundation, Vaddeswaram, AP,India.*
ORCID ID : 0009-0009-6373-4769
** Corresponding Author Email: bgvthm38@gmail.com*

powerful radio transceiver, an improved processor, and greater storage capacity. The patient's Data Aggregator (PDA) is a central component that consolidates the medical history and profile of every individual. Through this approach, the data collected by various sensor nodes are sent to the PDA. The PDA is a vital part of any healthcare system, as it collects and transmits medical data from various sensors. These data are then sent to a room controller, which then triggers alarms for the healthcare professionals in the remote facility. The goal of the transmission is to detect deviations in the monitored parameters, which can trigger alarms for medical professionals. On the other hand, a remote doctor can keep track of their patients' health status using a graphical interface.

Our overall architecture, as depicted in Figure 1, encompasses four different types of nodes: Sensor node (SN), PDA, Room Controller (RC), and Health care centre (HC).

Sensor Node (SN): The sensing nodes play a crucial role in the architecture as they are directly attached to the body of each patient to capture their health data. These sensor nodes consist of various components, including sensor hardware, memory, power unit, processor, and a transmitter [5]. Their primary function is to sense and collect relevant information from the human body, process it, and transmit the data to the Patient's Data Aggregator (PDA). Additionally, the sensors are capable of receiving requests to initiate specific sensing actions within the body.

Patient's Data Aggregator (PDA): The PDA is a central component of the architecture. It enables patients to manage their various health conditions. The device, which is attached to the bed of a patient, functions according to the information collected by its sensors. It then sends this data to the room controllers via the PDA. The PDA can keep track of the patient's health parameters and medical history, which makes it easy to retrieve this information when needed.

Room Controller (Rc): The room controller acts as a gateway or router that enables connectivity between the various patient-facing applications and the healthcare center. The room controller's node is an essential part of the data collection process for various PDA devices. The distribution and number of RC nodes depending on the size of the facility and its coverage requirements are set. These are usually placed at a certain location within the network.

Health Care Center (Hc): The data collected by the various room controllers is sent and received by the Hc central hub. This data is then stored in a database. The database allows the future processing of data and serves as a reference for individuals who are authorized to use it, such as family members and medical personnel. The data collected by the device is then stored in the database maintained by the healthcare facility.

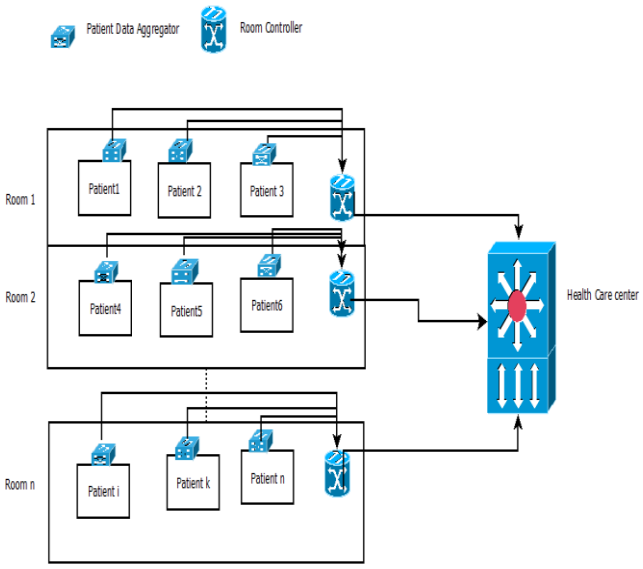

Fig. 1. Proposed Architecture for Medical WSNs.

2.1 Adversary Model

The security of networks is of utmost importance, especially when it comes to medical sensor networks. Confidentiality of data is essential. The data collected by medical wireless sensor networks are used in the diagnosis and treatment of patients. In order to ensure its reliability, this information must be protected from unauthorized access. Due to the unique features of medical wireless sensor networks, they are prone to security issues [13]. These include their limited computational capabilities, power consumption, and memory. Furthermore, MWSNs are prone to exploitation in unpredictable and open environments. Sensor nodes are typically placed in hostile environments, which can make them vulnerable to attacks [14].

An attack on a medical wireless sensor network can be categorized as an active or passive attack. The latter involves eavesdropping on the data collected by the sensor nodes. On the other hand, active attacks enable attackers to modify data, inject messages, or discard messages, among other actions. An example of a passive attack is when an attacker eavesdrops on wireless transmissions, potentially compromising the privacy of the patient's health information. In addition, it's possible for internal users to forge the data collected by the device. For instance, they can make fraudulent emergency calls or alter the values reported. Such actions could result in life-threatening medical interventions. [15].

2.2 Requirements of a secure system

This section aims to provide a framework for developing a lightweight and secure system for medical wireless sensor networks (MWSNs). The main objective of this system is to ensure that the data collected by the network is secure and efficiently transmitted between the sensor node and the healthcare facility [13–15]. Table 1 shows the system requirements of the proposed model.

Table 1: Security Requirements in the MWSN

Requirement	Description
Data Integrity	It is imperative to ensure the integrity of patient data during transmission.
Data Confidentiality	A secure mechanism should be implemented to ensure that only the intended recipient can access the data collected by the wireless sensor network. To achieve confidentiality, cryptographic methods are employed. These mechanisms encrypt the data, generating cipher text that ensures the confidentiality of the information.
Access control	It's also important to implement a strict policy that prevents unauthorized access to the data collected by the MWSNs.
Data Availability	In the realm of network security, availability refers to the continuous availability of secure communication services, even in the face of attacks such as Denial of Service (DoS) attacks. Similarly, in MWSNs, it is essential to ensure that patient data remains accessible even during DoS attacks.
Authentication	MWSNs can be equipped with two types of services: data authentication and node authentication. The former ensures that the information sent by the sensor is authentic, while the latter verifies the identity of the node. A medical sensor should also be able to prevent unauthorized access to the data by ensuring that the data items collected are not tampered.

3. Priority based Data Aggregation Method for MWSN

The purpose of this section is to introduce the concept of the PDMW system, which is a healthcare information aggregation system that enables providers to manage their patient data. In addition, we will discuss the details of the proposed scheme. The concept of the medical wireless sensor network shown in Figure 1 is designed to allow hospitals to monitor the health data of their patients. The network utilizes sensors attached to the body. The staff members at a medical facility can monitor various physiological parameters such as temperature, pulse rate, and ECG. The PDA is a vital component of the system that enables the transmission of data to the appropriate healthcare facility. It can also be utilized to make it accessible to the appropriate staff members, such as nurses and physicians. The complexity and varying characteristics of health information make it difficult to interpret. After conducting a comprehensive study, we have categorized it into three main categories: regular health data, emergency situations, and vital health data. Table 2 shows that the priority of delivering vital health data to the appropriate healthcare facility is highest during an emergency situation. This is because doctors require immediate delivery of this data to ensure that the patient is monitored continuously. On the other hand, regular data does not need to be delivered immediately and is not subject to the same urgency requirements. Doctors usually request the receipt of vital health data in order to keep track of their patients' conditions. This type of data should be sent to the HC prior to the next sensing period, though regular data does not require urgent delivery.

3.1 Data sensing

Healthcare applications that rely on medical sensors face energy constraints. While previous studies have shown that sensing operations consume less energy compared to radio communication, this assumption does not hold true for healthcare applications. In fact, sensing energy consumption can be comparable to, or even greater than, radio communication in such applications [16]. Additionally, the richness and growth of medical data over time can pose storage and transmission challenges, requiring excessive memory space [17].

To address these limitations, Trampled Sensing (TS) theory offers solutions. TS theory allows for a reduction in the sampling rate across the network, alleviating storage and transmission issues [18-19]. It has been demonstrated that sampling rates can be reduced to 30% and power consumption to 40% without compromising signal performance [21].

In the following sections, we will provide a concise explanation of the CS technique and its application in healthcare scenarios.

The compression technique is denoted with $x \in R^{L\times 1}$, where L is the length of the signal, and the compressed random row matrix is denoted with $\Phi \in R^{M\times L}(M << L, Rank(\Phi) = M),$ which is given as

$$y \in \Phi x \qquad (1)$$

Where the compressed data is represented with y and sensing matrix is represented with Φ, original data is represented with x.

3.2 Encryption process and Hashing Mechanism

Following the compression phase, the compressed data obtained through , Trampled Sensing (TS) is subjected to encryption. As the collected health data contain sensitive information crucial for medical diagnosis and treatment, it is essential to ensure its security. To address this concern, we propose an algorithm that dynamically updates individual keys each time a sensor transmits data. Researchers have observed that dynamic key updates provide a high level of security. In our proposed approach, we assume that the healthcare center (HC) holds the responsibility for generating, storing, and distributing the security parameters throughout the network. Below, we provide a detailed description of this algorithm, outlining its functioning and implementation.

The key pre-distribution algorithm from [24] is used in the proposed algorithm. During the deployment phase, a unique bivariate t-degree polynomial is assigned to both the Patient's Data Aggregator (PDA) and all sensor nodes. Each node is loaded with a distinct polynomial share over a finite field FP.

$$F_p : f(a,b) = \sum_{i=0}^{i=t} \sum_{j=0}^{j=t} c_{i,j} a^i b^j \quad (2)$$

Where P represents the largest prime number and it has the property of

$$f(a,b) = f(b,a)$$

The bivariate t-degree polynomial is securely maintained by the Healthcare Centre (H_C). The system utilizes two keys, namely K_j and K_i. The key K_j facilitates secure communication between the medical sensor and the Patient's data Aggregator (PDA). On the other hand, the key K_i enables secure communication between the PDA and the H_C.

Each sensor node S_{Nj} is assigned a unique polynomial share, represented as $f(S_{Ni}, y)$, which is securely stored and authenticated. Similarly, the Patient's Data Aggregator (PDA) is assigned a polynomial share, denoted as $f(PDA_i, y)$, where PDA_i represents the identity of the PDA. When a new sensor, such as S_{Nj}, is introduced to the Medical Sensor Network (MWSN), it receives a broadcast message containing PDA_i. Subsequently, SN_j computes the key K_j as $f(S_{Ni}, PDA_i)$ by evaluating the polynomial $f(S_{Ni}, y)$ at the value PDA_i.

SHA is a widely used security measure that ensures the integrity of data. It can also prevent unauthorized modifications. SHA-1 has a 20-byte output. On the other hand, SHA-2 has four hash functions that can be output in 256, 224, 384, and 512 bits. For instance, after carrying out 80 arithmetic operations, SHA-2 produces a 512-bit output. The proposed model uses the SHA-1 architecture [26].

The secure communication is carried out between the PDA and S_{Nj} using the key K_j. At round x, each sensor nodes $S_{N}j$ with the key K_j generates the ciphertext CT_j^x:

$$CT_j^x = (\{dt_j^x, x\}, k_j), h(dt_j^x, k_j) \quad (3)$$

Where dt is the compressed data by the sensor node, h(dt) is a hash value for the compressed data which is computed and transmitted to the PDA.

At the end of the x round , the kj for sensor node SNj is computed as

$$k_j^x = k_j^{x-1} \oplus h(dt_j^x) \quad x = 1,2,3...n \quad (4)$$

3.3 Proposed Priority Based Method for Data Aggregation

The encrypted data obtained from each sensor is transmitted to the Patient's Data Aggregator (PDA) for further processing. The PDA gathers all the encrypted information from the patient's sensors. The health data collected by these sensors can be classified into three main categories, as determined by medical wearable technologies (MWTs). These categories reflect different characteristics of the data, such as emergency situations or regular health information. It's important to note that health data may contain highly sensitive personal information, particularly in emergency scenarios.

Healthcare applications encounter the time constraint challenge, which necessitates the allocation of specific time intervals for each request. The nodes within the network determine the order in which the requests are sent based on these allocated time intervals. Alongside this, monitoring and managing the network traffic is also crucial to ensure smooth operations.

Our proposed prioritized data aggregation method is designed to minimize communication pipeline overhead and ensure efficient forwarding. Upon receiving the data, SN_j verifies the identity of each sensor involved. The collected health data undergoes authentication using K_j. The PDA takes charge of managing the network traffic based on the prioritized data. However, one drawback of this method is its inability to integrate with other data priorities, as each category requires distinct forwarding strategies. Nonetheless, packets within the same priority can be organized together for more streamlined processing.

At the time of execution, each PDA is communicated to the polynomial share f(x,y), and authenticated The key K_i is used to manage the confidentiality between the health center and PDA. In this section, we will discuss about the different forwarding strategies that are designed for the different priorities of data.

3.3.1 General Health Data

The packet generated at the time of general data with PDA is given as follows:

$$GD_i^x = E(\{P_i^x \| dt_i^x \| T), x\}, k_i), h(\{P_i^x \| Dt_i^x \| T\}), k_i)$$

Where Pix is the present condition of the patient, T is time stamp of the data, dt is the data transmitted to the PDA.

3.3.2 Emergency Condition:

The packet generated at the time of emergency condition with PDA is given as follows:

$$EC_i^x = E(\{P_i^x \| Loc \| T), x\}, k_i), h(\{P_i^x \| Loc \| T\}, k_i)$$

Where Pix is the emergency condition of the patient, T is time stamp of the data, Loc is the location of the patient. The PDA forwards the emergency packets directly to the health care centre.

3.3.3 Crucial health data :

The packet generated at the time of crucial data with PDA is given as follows:

$$CD_i^x = E(\{P_i^x \parallel dt_i^x \parallel T), x\}, k_i), h(\{P_i^x \parallel Dt_i^x \parallel T\}), k_i)$$

In the round x, the CD_i^x is the crucial data for P_i^x, in the next round the PDA only sends the difference between the dt_i^x and dt_i^{x-1}.

The PDA forwards the { $PDA_i(GD_i^x, EC_i^x, CD_i^x)$} to the health care centre. After receiving the packets generated by PDA, the H_c computes the Key $k_i = f(PDA_i, H_{Ci}) = f(H_{Ci}, PDA_i)$. Then the key k_i is used by the PDA to decrypt the packets. Also the key k_j is used by PDA to compute the hash function and verify the hash function received. Finally, the H_C access the data for diagnosis.

4. Experimental Analysis

The V2.0 electronic health sensor shield is specifically designed to automate the process of acquiring vital sign signals [27]. Within the medical sensor system, a network of sensors is strategically placed on the patient's body. These sensors enable continuous monitoring of the patient's health status. The collected data is then analyzed to provide accurate diagnoses and facilitate appropriate actions. The Arduino platform proves to be an excellent choice for developing medical and biometric applications that rely on sensor technology. A wide range of sensors, including a pulse oximeter, oxygen saturation sensor, blood pressure cuff, temperature sensor, glucometer, galvanic skin response sensor, ECG, and patient position sensor, can be incorporated into the system. These sensors are equipped with preprocessing and acquisition capabilities, enhancing their functionality and accuracy in capturing relevant health data.

The main advantage of the PDA over a medical sensor is its ability to provide users with unlimited resources and power. When choosing an embedded device, special considerations should be taken into account.

We have selected the Texas Instruments' CC2530 Development Kit [28], which includes a complete solution for implementing 802.15.4 applications. This includes a 2.4GHz radio frequency receiver, an 8051MCU microcontroller, 8 KB RAM, and a battery-powered ambient/environment device.

The kit includes two evaluation boards and three minimal boards. These components are equipped with a joystick, an RS-232 port, an LCD display, and a USB port. The health data collected by the medical sensor is sent to the healthcare center through the USB interface.

The proposed model is compared with the other existing algorithms such as CodeBlue [18], MobiCare[19] and UbiMon [25]. Figure 2 shows the execution time of proposed and existing algorithms. It is observed that the execution time of the proposed method is observed to be directly proportional to the size of the input blocks. When aiming for practical compression ratios within the range of 0.2 to 0.6, it is advisable to employ smaller frame sizes as a suitable design approach. The proposed method execution time is less compared against the existing algorithms.

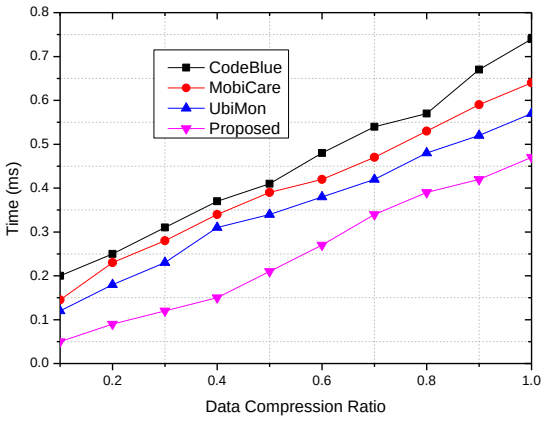

Fig. 2. Execution Time Data Vs Compression Ratio

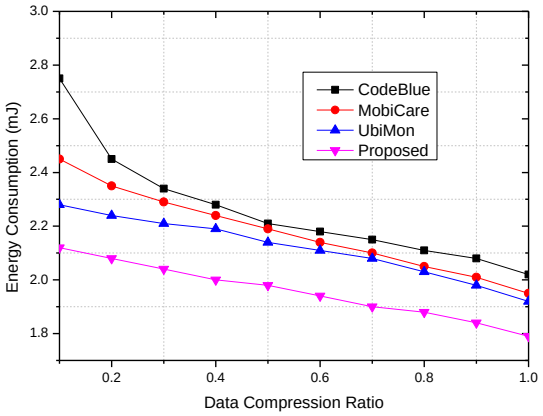

Fig. 3. Energy Consumption Data Vs Compression Ratio

Figure 3 depicts the energy consumption of the computational sensing component on the sensors. It demonstrates how lowering the compression ratios of the system can help reduce energy consumption. In all cases, having larger frames leads to lower absolute energy consumption. But, due to the increase in idle time, the system can achieve lower absolute consumptions through lower compression ratios.

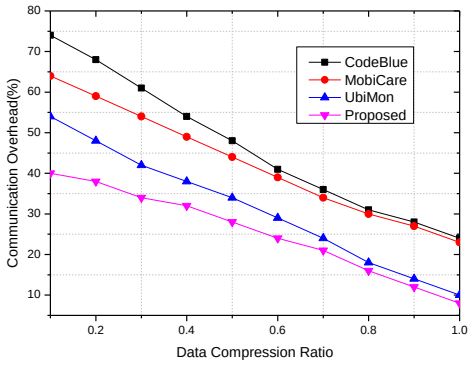

Fig. 4. Communication Overhead Vs Compression Ratio

Figure 4 shows the communication overhead of the proposed and existing system. The efficiency of this system is evaluated by considering the impact of computational sensing component on the overhead. The proposed system has a significant reduction in its communication overhead, as shown in Figure 4. This is due to the CS technique's ability to minimize the number of bits that are required for transmission. With higher data compression, fewer details must be hashed and encrypted, and they can be sent to the PDA. This means that the system can reduce its communication overhead by around 30 to 70%. The results indicate that compressive sensing significantly lowers the system's communication requirements. It should also be noted that there is a tradeoff between the performance of the system and the block sizes that are used.

5. Conclusion

Medical wireless sensor network (MWSN) is composed of devices that are equipped with wireless communication capabilities. These allow the collection of vital information from patients. The ability to monitor and analyze medical data through a wireless sensor network is a promising technology that can help improve the quality of care for patients and healthcare personnel. In this study we will focus on the aggregation of medical data in MWSNs and other wireless hospital networks. In this study, we focused on the creation of a prioritized data aggregation framework that aims to ensure the integrity of the collected information. This framework utilizes a combination of encryption and Compressive Sensing techniques to secure the collected information. In addition to this, we have conducted several experiments to evaluate the performance of the proposed system. The results of the experiments revealed the potential of the proposed framework to improve the efficiency of the wireless sensor network. In the future, we will explore the possibility of incorporating additional services that can further enhance the system's performance.

5.1. Appendix

Appendixes, if needed, appear before the acknowledgment.

5.2. Acknowledgment

The preferred spelling of the word “acknowledgment” in American English is without an “e” after the “g.” Use the singular heading even if you have many acknowledgments. Avoid expressions such as “One of us (S.B.A.) would like to thank ... .” Instead, write “F. A. Author thanks ... .” In most cases, sponsor and financial support acknowledgments are placed in the unnumbered footnote on the first page, not here.

6. References and Footnotes

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Lounis, Ahmed, Abdelkrim Hadjidj, Abdelmadjid Bouabdallah, and Yacine Challal. "Healing on the cloud: Secure cloud architecture for medical wireless sensor networks." Future Generation Computer Systems 55 (2016): 266-277.

[2] Agrawal, Vivek. "Security and privacy issues in wireless sensor networks for healthcare." In Internet of Things. User-Centric IoT: First International Summit, IoT360 2014, Rome, Italy, October 27-28, 2014, Revised Selected Papers, Part I, pp. 223-228. Springer International Publishing, 2015.

[3] Bhola, Jyoti, Surender Soni, and Gagandeep Kaur Cheema. "Recent trends for security applications in wireless sensor networks–a technical review." In 2019 6th international conference on computing for sustainable global development (INDIACom), pp. 707-712. IEEE, 2019.

[4] Prakash, Shiva. "An overview of healthcare perspective based security issues in wireless sensor networks." In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 870-875. IEEE, 2016.

[5] Internet of Things Global Standards Initiative”. ITU. Retrieved 26 June 2018.

[6] Natarajan, Rajesh, Gururaj Harinahallo Lokesh, Francesco Flammini, Anitha Premkumar, Vinoth Kumar Venkatesan, and Shashi Kant Gupta. "A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0." Infrastructures 8, no. 2 (2023): 22.

[7] Chiuchisan I, Dimian M. Internet of Things for e-Health: An approach to medical applications[C]//Computational Intelligence for Multimedia Understanding (IWCIM), 2015 International Workshop on. IEEE, 2015: 1-5.

[8] Ahmad, Rami, Raniyah Wazirali, and Tarik Abu-Ain. "Machine learning for wireless sensor networks security: An overview of challenges and issues." Sensors 22, no. 13 (2022): 4730.

[9] Saxena, Akash, DIPANKAR MISRA, R. Ganesamoorthy, Jose Luis Arias Gonzales, Hashem Ali Almashaqbeh, and Vikas Tripathi. "Artificial Intelligence Wireless Network Data Security System For Medical Records Using Cryptography Management." In 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 2555-2559. IEEE, 2022.

[10] Yang Y. Attribute-based data retrieval with semantic keyword search for e-health cloud [J]. Journal of Cloud Computing, 2015, 4(1): 1.

[11] J. Yang, J. Li, Y. Niu, ”A hybrid solution for privacy preserving medical data sharing in the cloud environment,” Future Generation Computer Systems. 2015, vol. 43-44, pp. 74-86.

[12] A. Abbas, S. Khan, ”A review on the state-of-the-art privacy preserving approaches in e-health clouds,” IEEE Journal of Biomedical Health Informatics, 2014, vol. 18, pp. 1431-1441.

[13] D. Singh, G. Tripathi, and A. J. Jara, ”A survey of Internet-of-Things: Future vision, architecture, challenges and services,” in Proc. IEEE World Forum on Internet of Things, 2014, pp. 287-292.

[14] Bernabe J B, Ramos J L H, Gomez A F S. TACIoT: multidimensional trust-aware access control system for the Internet of Things[J]. Soft Computing, 2016, 20(5): 1763-1779.

[15] Bae G, Shin K. An Efficient Hardware Implementation of Lightweight Block Cipher Algorithm CLEFIA for IoT Security Applications[J]. Journal of the Korea Institute of Information and Communication Engineering, 2016, 20(2): 351-358.

[16] Khemissa H, Tandjaoui D. A Lightweight Authentication Scheme for E-Health Applications in the Context of Internet of Things[C]. International Conference on Next Generation Mobile Applications, Services and Technologies. 2015.

[17] Yao X, Chen Z, Tian Y. A lightweight attribute-based encryption scheme for the Internet of Things[J]. Future Generation Computer Systems, 2015, 49(C):104-112.

[18] Malan D, Jones TF, Welsh M, Moulton S. CodeBlue: an ad-hoc sensor network infrastructure for emergency medical care. In Workshop on Applications of Mobile Embedded Systems (WAMES 2004), Boston, MA, USA, 2004; 12–14.

[19] Rajasekaran MP, Radhakrishnan S, Subbaraj P. Sensor grid applications in patient monitoring. Future Generation Computer Systems 2010; 26: 569–575.

[20] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, K. Fu, Plutus: Scalable secure file sharing on untrusted storage, in: Proceedings of the 2nd USENIX Conference on File and Storage Technologies, USENIX Association, Berkeley, CA, USA, 2003, pp. 29–42.

[21] Xu, Zhiyan, Debiao He, Pandi Vijayakumar, Brij Gupta, and Jian Shen. "Certificateless public auditing scheme with data privacy and dynamics in group user model of cloud-assisted medical wsns." IEEE Journal of Biomedical and Health Informatics (2021).

[22] Saleem, Muhammad Asad, Salman Shamshad, Shafiq Ahmed, Zahid Ghaffar, and Khalid Mahmood. "Security analysis on "A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems"." IEEE Systems Journal 15, no. 4 (2021): 5557-5559.

[23] Al-Zubaidie, Mishall, Zhongwei Zhang, and Ji Zhang. "REISCH: incorporating lightweight and reliable algorithms into healthcare applications of WSNs." Applied Sciences 10, no. 6 (2020): 2007.

[24] Velasco, Francisco Alcaraz, Jose Manuel Palomares, and Joaquin Olivares. "Lightweight method of shuffling overlapped data-blocks for data integrity and security in WSNs." Computer Networks 199 (2021): 108470.

[25] Yi, Fumin, Lei Zhang, Lijuan Xu, Shumian Yang, Yanrong Lu, and Dawei Zhao. "WSNEAP: An Efficient Authentication Protocol for IIoT-Oriented Wireless Sensor Networks." Sensors 22, no. 19 (2022): 7413.

[26] Nandhini, A. Sunitha, and P. Vivekanandan. "A novel security and energy efficient data aggregation for medical Internet of Things using trust." Journal of Medical Imaging and Health Informatics 10, no. 1 (2020): 249-255.

[27] Puranikmath, Veena I., Sunil S. Harakannanavar, Satyendra Kumar, and Dattaprasad Torse. "Comprehensive study of data aggregation models, challenges and security issues in wireless sensor networks." International Journal of Computer Network and Information Security 11, no. 3 (2019): 30.

[28] Memon, Muhammad Hunain, Muhammad Hammad Memon, Syeda Munazza Marium, and Jalaluddin Khan. "Security and privacy issues of medical systems in wireless sensor networks: A survey." Asian Journal For Convergence In Technology (AJCT) ISSN-2350-1146 5, no. 3 (2019): 08-12.