Wireless Sensor-Based Hashing Technique For Secure Patient Record Transferring In Biometrics System

S.Rajeswari[1*], S.A.Arunmozhi[2], Y.Venkataramani[3]

[1*,2,3]Department of Electronics and Communication Engineering, Saranathan College of Engineering, Trichy , TamilNadu, India

Email: rajeswaris-ece@saranathan.ac.in, arunmozhi-ece@saranathan.ac.in,deanrd44@gmail.com

[*]Corresponding Author

Abstract:

Over the past two periods, advancements in communication technology have exploded, with the last decade seeing an unprecedented explosion in the production of numerous cutting-edge, handheld and small communication devices. Modern, high-speed wireless communication technologies that employ complex network and communication protocols and standards have quickly supplanted the traditional wired scheme of communication. Wireless medical sensor networks are a promising application of WSNs in healthcare since they allow for remote patient monitoring (WMSNs). Reliable patient communication, patient mobility, and energy-efficient routing are at the forefront of current WMSN healthcare research developments. Nonetheless, patients' personal information is at risk when new technologies are implemented in healthcare applications without proper security measures being taken. In this study, we present a privacy-preserving strategy for the secure transfer of medical records over WSNs by combining secret sharing, and hashing. The healthcare information gathered by a wireless sensor network is broken down into subsets. In addition, a popular hashing algorithm is used to determine a unique identifier for each constituent. Any alterations to the message will result in a different hash value. Multipath routing is then used to send these parts to the servers. In order to verify the efficacy of the new method, this paper presents comprehensive simulations. The results indicate that secret splitting, in conjunction with multipath routing, aids in the maintenance of confidentiality in a wireless sensor network-based healthcare scheme.

Keyword: Privacy preservation, sharing, communication. Clustering, machine learning, encryption, wireless sensor networks.

DOI Number: 10.14704/nq.2022.20.11.NQ66051 **NeuroQuantology 2022; 20(11): 485-494**

1. Introduction

A WSNs are currently a topic of intense study because of their potential to drastically alter modern society. A WSN is the smallest unit in a network, and it has its own set of special properties, such as the ability to be deployed on a massive scale, to be mobile and reliable, and so on. WSNs have several applications outside of traditional engineering and science fields, including the military, water monitoring, infrastructure monitoring, government security policy, habitat monitoring, environmental monitoring, and seismic monitoring. Low-cost, low-power, low-memory, little-computative-power nodes that interconnect wirelessly over congested incidences with low bandwidth make form a sensor network [1]. The primary purposes of WSNs are to gather environmental data in an unattended region, send it to a base station, and analyse it. The unstructured information is then transferred to a distant server, where it undergoes either online or offline processing before being analysed in depth, depending on the needs of the

application. Military applications, area monitoring, environmental monitoring, sensing, monitoring, healthcare monitoring, etc. are just some of the many places where Wireless Sensor Networks (WSNs) find usage. WSN-based healthcare systems are made up of independent sensor nodes that can exchange data with one another wirelessly [2]. These nodes collect data on a variety of physical factors, including those related to motion, temperature, pressure, and more, in the studied region. The health care system is useful for keeping tabs on patients and keeping track of their illnesses. After examining the patients, the doctors recommend that they take certain measures for a set amount of time. Consequently [3], the elderly and others with varying degrees of disability can receive assistance in the comfort of their own homes thanks to the healthcare monitoring system. Patients' personal information should never be made public, for fear of abuse or because privacy concerns can prevent people from making full use of the technology. Even though Chakravorty admitted there were safety concerns with Mobile Care, he also said that fixing those problems wouldn't be enough for truly real-time healthcare software. In reality, the writer posited that patient privacy, data integrity, which is founded on the wireless transport layer security (WTLS) protocol. As a result, MobiCare healthcare monitoring still lacks security and privacy features, or they may have been left out in favour of future development [4].

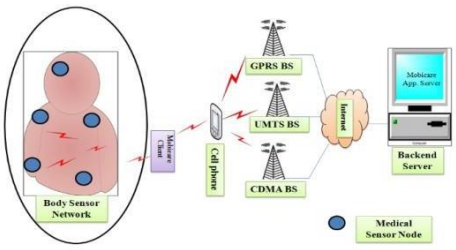

Figure 1: Mobi-Care patient monitoring architecture

Internet of Things, cyber-physical schemes, robots, and e-health are just a few examples of disruptive digital technologies that rely on readily available, low-cost, and simple-to-assemble parts. Conformably attachable, state-of-the-art biomedical devices are a prime example; these allow for precise monitoring of physiological and vital parameters, and are ideal for use on human skin [5]. Although many nano generators for wearable and implantable biomedical strategies have been obtainable, some of which also permit conformal contact to the, none of these solutions provide a facile, scalable, and cost-effective route to mass manufacturing that combines conformability [6], energy harvesting, and sensing. Integrating bendable energy-storage rudiments onto ultrathin substrates using spin coating or printing allows for a scalable solution for the simple realisation of bendable devices [7].

E-banking, internet shopping, medical insurance companies, etc., all acquire vast amounts of personally identifiable information about their customers. Information about a person that has been gathered and analysed digitally for a number of goals, such as scientific inquiry or commercial profit [8]. Personal data about specific people can be found in a micro dataset. As the need of privacy grows across disciplines, researchers are hard at work developing new methods to safeguard personal information. As such [9], there are several factors to take into account when conducting research on, or applying to, privacy-preserving data publishing. There are now two main types of research into the topic of privacy preservation. Privacy-Preserving are two such groups [10]. After using PPDM's data-mining features, your patterns can be kept secret from prying eyes.

Data can be created by individuals or organisations and gathered from a variety of channels to be analysed in a central repository. A data owner who want to expose their data to the public for research purposes may do so

after cleaning and combining their data. If intruders gain access to this information, they may use it in conjunction with other publicly available information to determine sensitive details about the target [11]. If this is the case, the solution is for the data owner to provide masked data that protects individual privacy while still allowing the data to be useful. The individual's privacy may still be compromised if this camouflaged data were combined with other sources. PPDP is a method of solving such problems such that sensitive information is safe from prying eyes [12]. Data protection through design (PPDP) refers to the procedure of creating safeguards for existing information. Publishing data makes it simple to share and trade information. Controlled information dissemination is used to define the concept of privacy. When it comes to sharing private information, privacy controls who may see it and how it can be used. Data privacy protection is intended to be a prerequisite for making good use of the data. Electronic storage of the information makes it inaccessible to any particular person. When it comes to data publishing, anonymization is the essential method for ensuring individual privacy.

2. Related works

This section begins with the essential background knowledge on the application of WSN with implantable electronic devices as well as providing an introduction to the latest techniques being used for patients worldwide. The exciting opportunities to adapt and influence implantable sensors to enrich the preclinical development have been outlined. The conceptual illustration of generic biomedical implantable electronic system and biomedical telemetry system has been delineated. The most important methods of powering implantable devices have been comprehensively reviewed. The merits and demerits of each method have been illustrated to identify the suitable method to power subcutaneous implanted devices. Lightweight middleware was proposed by Waluyo et al. [13]. The suggested middleware's goal is to use highly reusable codes to streamline and quicken the process of creating wireless healthcare apps. Features of the middleware architecture include data gathering, dynamic sensor reconfiguration, plug-and-play adaptability, and resource management. Important sensor data is encrypted to prevent access by unauthorised parties. For privacy, the authors rely on the 622 byte ROM-intensive Skip Jack 64-bit lightweight block cypher cryptosystem. Three one ECG were used for the performance analysis. The proposed middleware is implemented as PDA software (PDA).

Protected entry was proposed by Huang et al. [14] to a healthcare monitoring architecture based on a hierarchy of sensors. There are three main ubiquitous healthcare applications that have been shown to work with the healthcare architecture's three network tiers. A wearable equipped with Bluetooth and biomedical sensors is used to track physiological signals in the sensor network layer. There are wireless sensor nodes (i.e. Mica2) dispersed throughout the structure that measure various environmental variables. Wireless sensor networks (WSS) and wireless sensor networks (WSM) safely transmit environmental and physiological data to higher layers. Point-to-point communication between two WSM swarm nodes is encrypted using a polynomial-based encryption approach in WSMs, whereas in WSS, authentication and encryption are handled using an AES-based CBC-MAC scheme.

The MAACE protocol, established by Le et al. [15], allows for a qualified medical expert to view a patient's records. Their elliptic curve cryptography-based method allows for two-way authentication and access control (ECC). What's more, the authors assert that their approach is immune to real-time attacks

including replay attacks and denial-of-service attacks. A sensor network, and data access layer make up the MAACE architecture (DA). The SN sends information to the CN (a personal digital assistant, laptop, or mobile phone), which then sends it on to the DA for archival purposes. While the security provided by the protocol developed by Le et al. is sufficient, there is a risk that sensitive patient data could be compromised due to information-leakage attacks. This is unacceptable for real-time healthcare applications since it leaves the patient's vital signs open to prying eyes. Using wireless sensor networks, Haque et al. [16] established a robust security architecture for patient monitoring systems. Three essential players—the patient (PT), the healthcare service system (HSS), and the secure base stations—make up their public-key-based system (SBSs). Secure communication between HSS and SBS or PT and SBS is established by the use of a bilateral key handshaking method and a pair-wise shared key derived using a pseudo-inverse matrix. Any PT node in the network can initiate secure communication with the SBS, because the SBS already knows the secret keys of the PTs and HSSs. In addition, their method ensures the privacy of the collected information (i.e., encryption and decryption).

Medical wireless sensor networks are the basis of the secure health monitoring (SHM) system suggested by Kumar et al. [17]. SHM protects the privacy, veracity, and correctness of medical records while minimising their storage, transfer, and processing overhead. The components of the proposed approach are (a) low-power; and (b) the capacity to detect ECG signals wirelessly within the patient's body. PingPong-128 stream cypher encryption is used to ensure privacy in SHM, whereas Ping-Pong-MAC (short for message authentication code) is used to ensure the authenticity and integrity of messages. The suggested SHM also has low resource requirements, requiring only 19.2 milliseconds of CPU time and 1.1 kilobytes of RAM.

3. Problem Statement

Cryptography is an important technique to ameliorate the security of data in sensor networks and it is provided by the process of encryption and decryption, in which the keys are exchanged among the nodes to convert the cipher text to a readable form. Sharing the keys via malicious nodes may cause disclosure of keys to the attackers. The existing frameworks use several techniques and protocols to achieve high security. The traditional cryptography techniques suffered from several issues such as more execution time and energy consumption. Further, they did not achieve a high level of security. Although so much work has been done in this field, but still there is a need of new hybrid cryptography algorithm. Moreover, hash functions are used to provide data integrity. Recent attacks such as brute-force attacks and crypt analytical attacks on standard hashing techniques encourage researchers to design new hashing techniques. Existing hashing techniques have setbacks including more execution time and large digest size. There is a need to improve the existing hashing techniques.

4. Proposed Architecture

For example, in Fig.2 we see the Architecture of Multipath Splitting and Renovation with Hashing, where denotes the unique size of the message being transmitted. Hashing is used to protect communication channels from outside interference. This is why there are three sections in the original message. These message streams and their associated hash values are transmitted across servers in the direction of the receiver, where they are combined to recreate the original message. At first, M's message was split into three sections:,, and. These partitioning devices send message streams and their associated hash values to remote servers. The message and its hash value are subsequently sent to the server. moves data from the sending node to the

receiving node. From the sending node to the receiving server, the stream of messages is sent. In a similar vein, the destination nodes send and receive hashed messages and servers. This server processes incoming messages and translates the hashed input message. Results from the server and client are and, respectively, which are then sent to the receiver. The servers send the data to the point of reconstruction, where the message is reconstructed.

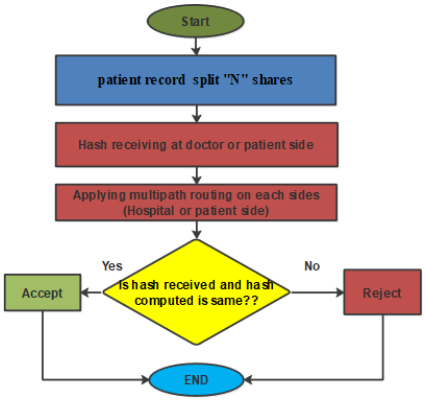

Figure 2: Construction of Multipath Modernization with Hashing

The first message branched off into individual pieces. These "n" shares switched to sending data through several paths. Hash function computation using multi-hop routing at the receiver end is also possible. The share and the hash function used on it are transmitted to the receiver during the reconstruction stage. Then, compare the received share count to the count obtained before and after hashing. If yes, then the message is accepted; if not, the message is declined.

5. Security and Privacy Requirements of Healthcare Applications

This section highlights the most important security and privacy necessities for healthcare applications utilising WSN, taking into account the aforementioned use cases, security concerns, and regulatory laws:

Data confidentiality: Confidentiality of patient health information is required by law and medical ethics. Only authorised medical professionals should be allowed to access these records. To prevent an enemy from eavesdropping on a patient's information, it is crucial to preserve the confidentiality of the patient's health records. It's possible for the patient's safety to be compromised due to data eavesdropping because the adversary can exploit the patient's data for various nefarious objectives. As a result, protecting the privacy of patient information is crucial for WMSN-based healthcare applications.

Data authentication: Authorization is required for both medical and non-medical uses, and this is what authentication services provide. To ensure only reliable sensors are sending data to the base station, authentication on both ends is required in WMSN healthcare applications.

Patient permission: In order to share a patient's health records with a healthcare consultant, a healthcare professional must first obtain the patient's consent. The medical research community, insurance agencies, etc. In addition, since medical sensor networks are generally wireless in design, patient anonymity is a must for healthcare applications. The anonymity provided by wireless communication ensures that the origin of a packet (such as data from a medical sensor) remains concealed. It's a service that can make privacy possible. A application must also be able to survive at least some power outages, malfunctions, or attacks.

6. Hashing Technique

Hash function has two elements: compression function, which converts arbitrary size input into fixed size output; and a construction function, which calls compression function repeatedly to process a message.

Design of Projected Hashing:

Step 1: Padding- Padding of bits 1 and then 0 is done, such that the length of message after padding is congruent to 448 modulo 512 (length ≡ 440 mod 512).

Step 2: Attaching- After padding, append the length of original message in 64

bit representation, so that the length of message is now in multiples of 512.

Step 3: Message into Blocks- The message gotten from the previous step is

divided into n Blocks of size 512 bits. That is:

$B0, B1, B2, B3, B4, B5, B6, B7, \ldots\ldots\ldots\ldots Bn$

Step 4: Subdividing Blocks Into Larger Ones. Each new block you create using a larger one you receive from the preceding one. Step 2: Split the Blocks into 128-Bit Sub-Blocks.

That is:

$(\mathrm{B01}, \mathrm{B02}, \mathrm{B03}, \mathrm{B04}), (\mathrm{B11}, \mathrm{B12}, \mathrm{B13}, \mathrm{B14}),$
$(\mathrm{B21}, \mathrm{B22}, \mathrm{B23}, \mathrm{B24}), \ldots\ldots\ldots\ldots\ldots\ldots$
$(\mathrm{Bn1}, \mathrm{Bn2}, \mathrm{Bn3}, \mathrm{Bn4})$

Step 5:Next, we'll apply the XOR operation, which involves summing up the values of all the blocks' subparts and replacing the resulting value with that total. Since each sub-block is 128 bits in size, the resulting block size after XOR operation is also 128 bits. Which means:

$\mathrm{B0} = \mathrm{B01\ XOR\ B02\ XOR\ B03\ XOR\ B04}$

$\mathrm{B1} = \mathrm{B11\ XOR\ B12\ XOR\ B13\ XOR\ B14}$

$\mathrm{B2}$

$= B21\ XOR\ B22\ XOR\ B23\ XOR\ B24 \ldots.$

$\ldots\ldots\ldots and\ so\ on$

Step 6: The 128-bit block size achieved by the final XOR operation is the result of this process. Now we'll finish off by applying XOR to each block. A 128-bit message digest is the result.

$output = B0\ XOR\ B1\ XOR\ B2\ XOR\ B3$

Hashing and Message Digest

Hash tables are the foundation of the hashing technique, which is used to perform searches efficiently. A hash table is a type of data structure that stores associations between keys and their corresponding values. Hash tables provide for fast searching, and hence, quick inserting and removing, albeit at the cost of processing performance. At the outset, there is a piece of text (the key) that is fed into a hashing algorithm. A hash function, in its most basic form, is a generator for a function that accepts a hash table as an array as its input. If the hash table size is, then the indices will be. The result of applying a hash function to a key yields an index into a hash table or the key's physical location. In order to use hashing for searching, we need a function in which k represents a key and each of the integers in where, size of the hash of the key all equal each other.

Secret Sharing Requirement

This method allows for precise regulation and removes the possibility of a weak spot. No matter how hard an investor tries, he or she will never be able to alter or access the information.

Secure Routing

It may be necessary for sensor equipment to transmit data to other devices that are out of radio range, such as in home care or catastrophe circumstances. Therefore, end-to-end communication relies heavily on the services provided by routing and message forwarding. Numerous routing protocols for sensor networks have been proposed; however, none of them have been developed with robust security as a primary concern. There are a number of security holes in routing protocols, such as the possibility of a denial-of-service attack. An adversary can potentially introduce routing discrepancies by injecting malicious network. In addition, healthcare applications necessitate mobility supported routing protocols, although most existing approaches are geared for static wireless sensor networks

Shamir Secret Splitting

Discreet communication is a method that characterises confidential delivery. In this case, the contributors are those with proper permissions to view the information. Only when the various pieces of the secret are brought back together does the whole thing make sense.

Secret Sharing Requirement

This method allows for precise regulation and removes the possibility of a weak spot. No matter how hard an investor tries, he or she will never be able to alter or access the information.

Working of Shamir secret scheme

The Shamir system for exchanging secret information has many iterations. In this case, we employed a Shamir secret-sharing technique based on a threshold. The special participant, sometimes known as the group leader, is the one who can calculate the value of, so let's suppose and are positive integers. A leader's main responsibility is to surreptitiously disseminate knowledge to all members of the group. The term "threshold scheme" is commonly used to describe this method. Since we want to use a threshold method to distribute our secret in a situation where (h, m), all members are required for the rebuilding of the secret at the same time,

$$f(y) = a_0 + a_1 y + a_1 y^2 + \cdots . a_{k-1} y^{k-1}$$

Let's use an example to describe the Shamir secret so that the ideas are clearer. Let it be a mystery: where exactly does the node in the wireless medical sensor network store the information it collects? Further For the sake of argument, let's say that S. Equation (below) displays the polynomial.

$$f(y) = 1441 + 150y + 60y$$

Points of secret sharing (1441, 1.331, 1.551). The share for each of the participant is couple.

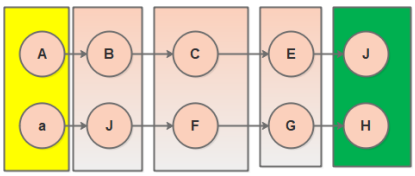

Figure 3: Routes achieved for multipath routing

Figure 3 represents is the Computing numerous pathways from a source node to a terminus node is an essential part of multipath routing [19]. In order to improve the network's dependability, these paths must be independent of one another. In this section, we extend the notion of a WSN-based healthcare system to a network where the vertices are nodes and vice versa. If we have a graph with vertices and, we can use Menger's theorem to prove that no two vertices in the graph are next to one another.

Properties of Hashing

Hash tables are mathematical functions that reduce the size of messages from a range to a constant. There are four distinct features of a hash function:

- One such function is the hash function (H), which takes as input a message of variable length and returns a value known as the message digest.
- Since the converse of h(x)=y cannot be calculated, we cannot easily determine what h(x) means.
- This scenario, along with others like "find y is not equals to x," gives rise to the term "poor collision resistance," which means that hashing both functions is computationally inefficient.
- In this case, it is possible to find a pair where the hashing function of is equal to the function of yh=(x=y), leading to the emergence of the phrase strong collision resistance.

7. Result and Simulation

The R2017b simulator in MATLAB will be utilised to carry out the investigation. When it comes to computing analysis that regulates signal processing communications and other sectors, MATLAB is by far the most popular choice. Matrix-lab, or MATLAB, is an acronym that combines the terms matrix and laboratory. Matrix manipulation, graph plotting, algorithm implementation, UI design, image processing, and interfacing with programmes written in other languages are all possible with this platform. When a secret key is taken into account, we have simulated an environment suitable for Shamir's sharing protocol. Using a plot of a polynomial function or the sent signal,

we may determine the range of values 1131. For the same range of values of, the received signal after reconstruction is also shown. It is evidence of the success of the reconstruction method that the reconstructed signal overlaps the original transmitted signals..

Table 1: Reconstructed and Splitting

S. No.	Shamir's Secret Sharing Scheme			
	Splitting Reconstruction			
	D	x	F(x)	
1	D-0	1	1441	
2	D-1	2	1621	D-1
3	D-2	3	3111	
4	D-3	4	2861	D-3
4	D-4	4	2148	D-4
5	D-5	5	2482	

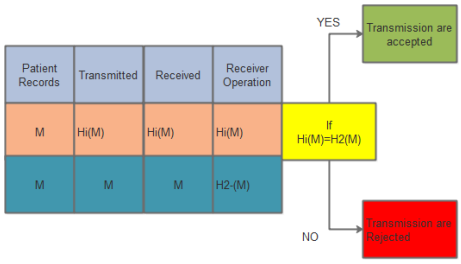

Figure 4: Reconstructed with Hashing technique

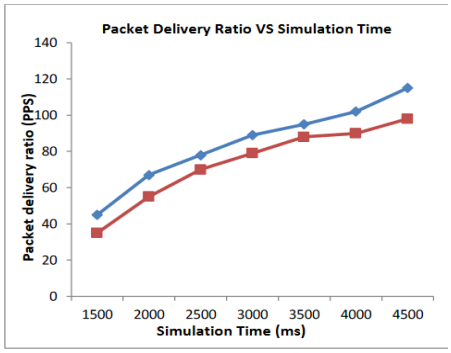

Figure 5: Packet Delivery Ratio

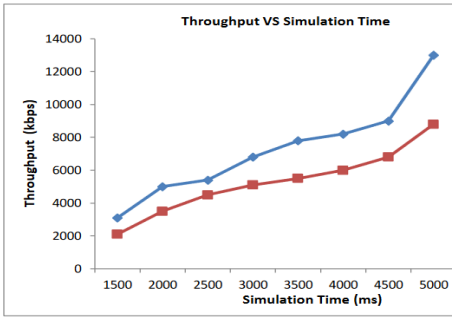

Figure 6: Throughput

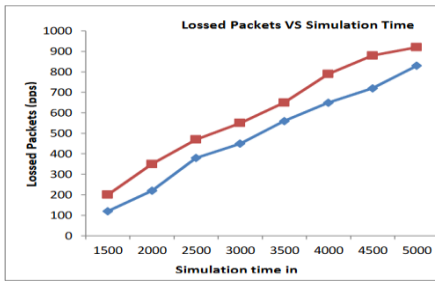

Figure 7: Communication Cost

The performance of the proposed work is calculated by using the following metrics on the above figures. On destination amount of received packets which is sent from the source node. And Throughput, as in random networks, is the rate at which information is transmitted in a linear fashion along a given channel. In addition, we calculate the typical delay, or how long it takes for a set number of packets to travel between a sender and a receiver. As a last step, we determine how much energy is typically allocated toward data processing, sleeping, monitoring, and transmitting.

8. Conclusion

While medical sensor networks in healthcare applications have numerous useful applications, they also pose hazards to patients' privacy and security. Thanks to technological advancements, medical records may now be transmitted digitally over the internet, paving the way for telemedicine. On the other hand, information might be deceptive. That's why safeguards against its inappropriate use are obligatory. Hashing is an easy method for protecting the confidential data in a transmission. In this study, we take a novel approach to improving the safety of health data by transmitting it through several independent channels. Using hashing, it is simple to check if a message has been authenticated after it has been received. Hashing is a great tool for ensuring the confidentiality requirements are met. The suggested approach involves slicing the original message into three pieces before sending each

of those pieces, together with the hash value, to their respective servers using multipath routing. To improve transmission safety, the multipath routing method is put into place. When comparing this scheme's outcomes to those of a plaintext transmission in a WSN-based healthcare system, the latter comes out on top.

References

[1] Anitha S, Jayanthi P, Chandrasekaran V. An intelligent based healthcare security monitoring schemes for detection of node replication attack in wireless sensor networks. Measurement. 2021 Jan 1;167:108272.

[2] Malik MS, Ahmed M, Abdullah T, Kousar N, Shumaila MN, Awais M. Wireless body area network security and privacy issue in e-healthcare. International Journal of Advanced Computer Science and Applications. 2018;9(4).

[3] Pundir S, Wazid M, Singh DP, Das AK, Rodrigues JJ, Park Y. Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges. IEEE Access. 2019 Dec 30;8:3343-63.

[4] R. Sowmyalakshmi, Mohamed Ibrahim Waly, Mohamed YacinSikkandar, T. Jayasankar, Sayed Sayeed Ahmad, Rashmi Rani and Suresh Chavhan, “An Optimal Lempel Ziv Markov Based Microarray Image Compression Algorithm”, Computers, Materials & Continua, vol. 69, no.2, pp. 2245-2260, 2021, ISSN: 1752-1767.

[5] Tsai KL, Leu FY, Tan JS. An ECC-based secure EMR transmission system with data leakage prevention scheme. International Journal of Computer Mathematics. 2016 Feb 1;93(2):367-83.

[6] Kumar, P. and Lee, H.J., 2011. Security issues in healthcare applications using wireless medical sensor networks: A survey. sensors, 12(1), pp.55-91.

[7] González FC, Villegas OO, Ramírez DE, Sánchez VG, Domínguez HO. Smart multi-level tool for remote patient monitoring based on a wireless sensor network and mobile augmented reality. Sensors. 2014 Sep 16;14(9):17212-34.

[8] C. Rajinikanth, P. Selvaraj, Mohamed YacinSikkandar, T. Jayasankar, SeifedineKadry and Yunyoung Nam, “Energy Efficient Cluster Based Clinical Decision Support System in IoT Environment”, Computers, Materials & Continua, vol. 69, no.2, pp. 2013-2029, 2021, ISSN: 1752-1767 (Print) 1546-2226.

[9] Wahyuni R, Rickyta A, Rahmalisa U, Irawan Y. Home security alarm using Wemos D1 and HC-SR501 sensor based telegram notification. Journal of Robotics and Control (JRC). 2021 May 5;2(3):200-4.

[10] J.JeanJustus, T.Jayasankar,G. Sheryl Oliver,C. Bharatiraja, N.B. Prakash,” Denaturalized cluster organization based improving energy constraints using relay link chain routing protocol in wireless sensor network," Journal of Ambient Intelligence and Humanized Computing (2020), ISSN: 1868-5137 (Print) 1868-5145

[11] Kumar A, Gyanchandani M, Jain P. A comparative review of privacy preservation techniques in data publishing. In2018 2nd International Conference on Inventive Systems and Control (ICISC) 2018 Jan 19 (pp. 1027-1032). IEEE.

[12] Agarkar A, Agrawal H. A review and vision on authentication and privacy preservation schemes in smart grid

network. Security and Privacy. 2019 Mar;2(2):62.

[13] Waluyo, A.B.; Pek, I.; Chen, X.; Yeoh, W.-S. Design and Evaluation of Lightweight Middleware for Personal Wireless Body Area Network. Pers. Ubiquit. Comput. 2009, 13, 509-525.

[14] Huang, Y.M.; Hsieh, M.Y.; Hung, H.C.; Park, J.H. Pervasive, Secure Access to a Hierarchical Sensor-Based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks. IEEE J. Select. Areas Commun. 2009, 27, 400-411.

[15] Le, X.H.; Khalid, M.; Sankar, R.; Lee, S. An Efficient Mutual Authentication and Access Control Scheme for Wireless Sensor Network in Healthcare. J. Networks 2011, 27, 355-364.

[16] Haque, M.M.; Pathan, A.S.K.; Hong, C.S. Securing u-Healthcare Sensor Networks Using Public Key Based Scheme. In Proceedings of 10th International Conference of Advance Communication Technology, Pyeongchang, Korea, 19–22 February 2008; pp. 1108-1111.

[17] Kumar, P.; Lee, Y.-D.; Lee, H.-J. Secure Health Monitoring Using Medical Wireless Sensor Networks. In Proceedings of 6th International Conference on Networked Computing and Advanced Information Management, Seoul, Korea, 16–18 August 2010; pp. 491-494.