

Research Article

Efficient Compression Sensing Mechanism Based WBAN System Using Blockchain

Vinay Pathak,¹ Karan Singh,¹ Radha Raman Chandan,² Sachin Kumar Gupta ,³ Manoj Kumar ,^{4,5} Shashi Bhushan ,⁶ and Sujith Jayaprakash ⁷

¹School of Computer and System Sciences, Jawaharlal Nehru University, New Delhi 110067, India

²Department of Computer Science, School of Management Sciences (SMS), Varanasi 221011, UP, India

³School of Electronics and Communication Engineering, Shri Mata Vaishno Devi University, Katra, Jammu and Kashmir, India

⁴Faculty of Engineering and Information Sciences, University of Wollongong, Dubai, UAE

⁵MEU Research Unit, Middle East University, Amman 11831, Jordan

⁶Department of Computer Science & Engineering, Amity University Punjab, Mohali, Punjab, India

⁷BlueCrest University College, Accra, Ghana

Correspondence should be addressed to Shashi Bhushan; tyagi_shashi@yahoo.com and Sujith Jayaprakash; sujith.jayaprakash@bluecrest.edu.gh

Received 13 October 2022; Revised 9 January 2023; Accepted 31 January 2023; Published 11 May 2023

Academic Editor: Shah Nazir

Copyright © 2023 Vinay Pathak et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The hybrid wireless sensor network is made up of Wireless Body Area Network (WBAN). Generally, many hospitals use cellular networks to support telemedicine. To provide the treatment to the patient on time, for this, an early diagnosis is required, for treatment. With the help of WBANs, collections and transmissions of essential biomedical data to monitor human health becomes easy. Compressor Sensing (CS) is an emerging signal compression/acquisition methodology that offers a protruding alternative to traditional signal acquisition. The proposed mechanism reduces message exchange overhead and enhances trust value estimation via response time and computational resources. It reduces cost and makes the system affordable to the patient. According to the results, the proposed scheme in terms of Compression Ratio (CR) is 18.18% to 88.11% better as compared to existing schemes. Also in terms of Percentage Root-Mean-Squared Difference (PRD) value, the proposed scheme is 18.18% to 34.21% better than with respect to existing schemes. The consensus for any new block is achieved in 24% less time than the Proof-of-Work (PoW) approach. The shallow CPU usage is required for the leader election mechanism. CPU utilization while the experiment lies in the range of 0.9% and 14%. While simulating a one-hour duration, the peak CPU utilization is 21%.

1. Introduction

One of the most critical industries that blockchain can change is healthcare: health records are currently stored in various places, and several private companies control them. Patients' medical records might be conflicting or misplaced. All those issues could be solved by using blockchain. Blockchain allows the creation of complete, accurate, and transferable healthcare information, giving individuals more control of their data without an intermediate party [1, 2]. Clinical trial management is another possible use of this technology: test results from clinical trials can now be compiled and distributed to researchers and experts cheaply and efficiently. The authenticity

of this information can also be insured due to the relative immutability of the blockchain. Strong clinical trial management results in more awareness about medical product purchases and a faster rate of scientific research. e-healthcare is a domain where continuous monitoring and gathering of the physiological signal and vitals tracking and recording is going on, which results from colossal data generation. In this entire process, data are accessed and disseminated regularly.

Every application is different and needs to have a separate security scheme depending on the application requirements. When it comes to WBAN, two issues get associated with it. First, WBAN is resource-constrained, and second, data transmission in WBAN must be secure. Keeping in view that

WBAN is a resource-constrained entity; all data transmission should be secured. WBANs mostly deal with the healthcare application, where a minor data alteration could be a threat to human life. So a lightweight security scheme that is compatible with resource constraint WBAN and can provide security. The conventional CS framework problem is that they do not provide enough compression ratio and the quality after reconstruction is relatively low in case of physiological signals [3]. This mostly happens due to model inaccuracy, and variability of the individual is being overlooked. CS helps in acquiring sparse or compressible signals. By definition of sparsity, to represent the information contained by signal, only a few significant components are sufficient instead of total signal length [4]. Similarly, the signal is said to be compressible if there is a rapid decay in the sorted components of the signal. Traditional methods for acquiring sparse signals use the Nyquist criterion. Samples generated by Nyquist criterion are too many, out of which only a few samples are retained having larger coefficient and discard the smaller coefficient samples. The signal containing the component having the highest frequency decides the rate of sampling using Nyquist-criterion. However, signal sparsity played a decisive role in the sampling rate of CS. This work includes the better performance of sensor chips through EEG by using a compressing sensing technique to receive better patient information, especially for Parkinson's disease [5].

This study, proposes a novel technique to help Parkinson's disease patient be monitored by the health centre and take fast action in an emergency case by adapting IoT technology with Compressive Sensing (CS) method. The contributions of this work can be listed as follows:

- (i) Design smart healthcare communication system for brain signal analysis.
- (ii) Collect, compress, and encrypt EEG signals using the CS method.
- (iii) Compressed data are decompressed and decrypted by the clouds, and then cloud analyses the data and makes a decision.

The proposed method shows that the results are promising in terms of CR and PRD. Results also demonstrate that the proposed scheme is suitable for constrained or edge device that have limited computational resources. This is a huge benefit to the citizens residing in remote areas.

The rest of the research paper organization is as follows: In Section 2, the proposed methodology is discussed with its different phases along with its applications. Section 3 shows the results of our method with comparative analysis with other existing schemes while in Section 4, the conclusion is discussed.

2. Literature Review

Memedi et al. has proposed [1] a scheme for patients with Parkinson's disease, helping them manage their symptoms. They have designed an architecture, which has an interface in between an electronic device and a patient. These sensors help collect some information to respond to

their mealtime, sleeping time, or exercise duration. Then stored data are saved into the data storage and an interface in between the patient and clinicians (expert in health-care). It could only store the data, which may not contain the symptoms or record symptoms of such patients. To collect the data from different devices is easy, but to store the data and detect the symptoms are issues to explore further study. Apart from this collection, the physiological wave storing them and transmission involve enormous energy because of the mechanism used to cater to the needed requirements [2]. Apart from this, the existing or traditional healthcare system is fixed and location-specific or stringent to geo-location. The main drawback of the existing system of disadvantage is associated with it because of wired pieces of equipment and wired biomedical sensor. The wired biomedical sensor's advantage is that they do not have power or energy, storage constraints. However, they restrict patients' mobility as per Ontario's [6] the cost of hospitalization is increased significantly because of the increase in elderly age people in coming future. Now it is the right time to think of to minimize the hospitalization cost and time. That is why existing hospitalization infrastructure needs to enhance mobility and provide wireless sensor-equipped infra to patients. So it is indispensable to reduce the load of sampling, transmission of the enormous quantity of data, security overhead, etc. WBANs transmission of information or data wirelessly, which is the very prone interception and eavesdropping in this era because of the number of cyber-attack noticed days today. Security problem significantly affects the development of WBANs because privacy is required by the Health Insurance Portability and Accountability Act [7]. Traditionally, the security aspect is dealt with or approached by using Advanced Encryption Schemes (AES) [8] with Diffie Hellmen Key Algorithms [9]. These two provide perfect security, but designs for equipment have abundant resources but AES overburden and shorten network lifetime because of substantial memory and computational power. Security has always been an area of research in every application. One generalized security scheme is not capable enough to provide security to all different types of applications.

2.1. Problems in the Existing Schemes. Apart from this, the existing or traditional healthcare system is fixed and location-specific or stringent to geo-location. The main drawback of the existing system of disadvantage is associated with it because of wired pieces of equipment and wired biomedical sensor. AES and DES provide perfect security but designed for the equipment that have abundant resources. AES overburden and shorten sensor network lifetime because of substantial memory and computational power. Security has always been an area of research in every application. One generalized security scheme is not capable enough to provide security to all different types of applications. Blockchain has been used in the proposed approach to maintain the security standards while reducing the overhead cost significantly.

3. Proposed Methodology

The objective of proposed methodology is to deliver efficient data transfer in between WBAN device and healthcare system server. The proposed mechanism is using compression sensing to reduce the data size and to relief WBANs node. The input data are taken from the EEG of Parkinson's diseases patient. This proposal creates a real scenario with the help of Arduino board. The main components of proposed work are data collection, compression, and transformation. In this section, the proposed solution aims to help Parkinson's disease patient that has to be monitored by the health centre and take fast action in an emergency case. The proposed data-driven compression sensing can compress various types of physiological signals by using the data encoding scheme. CS only considers a few random samples, which are used to acquire signals. The measurements in CS does not learn from the previous measurements, i.e., they are nonadaptive. As a result, the generated compressive measurements are relatively less and transmitted or stored quite easily. The steps involved in the proposed scheme are shown in Figure 1.

In Figure 1, to increase the accountability, security, and transparency all the transactions and flow offers blockchain as service. So, here the signal is compressed while acquiring and is named as compression sensing. CS meets all the requirement of a resource-constrained WBANs and also provides lightweight security. This solution, utilizes the properties of compression sensing for optimum use of the device's energy or resources. It prolongs the network lifetime and besides secures the network. The integration of compression sensing achieves additional power saving by reducing computation steps [10].

The proposed scheme consists of four phases: data collection, local process, data compression and encryption, and data analysis phase. During the data collection phase, the EEG sensor collects the brain data and sends it to the local processor. The local processor collects the data and decides either sending to the cloud or depending on pre-defined conditions and after that uses Compressive Sensing (CS) method to compress and encrypt the data. Finally, the compressed data are decompressed and decrypt by the clouds and then cloud analyses the data and make a decision.

3.1. Phases of the Proposed Scheme. The proposed scheme is divided into different-different phases based on their work type. All the phases are as follows with their brief explanation.

3.1.1. Data Collection Phase. This phase aims to collect the synapse signals that can be defined as electrical impulse signals sent from all body through the nerves. For this purpose, it uses EEG sensors, which decode those signals over the brain part and send them to the local processor.

EEG sensor attached to the patient head, and then it collects the signals, as shown in Figure 2. In this process, there is a device which has a particular type of EEG sensor that continuously collect the physiological signal generated

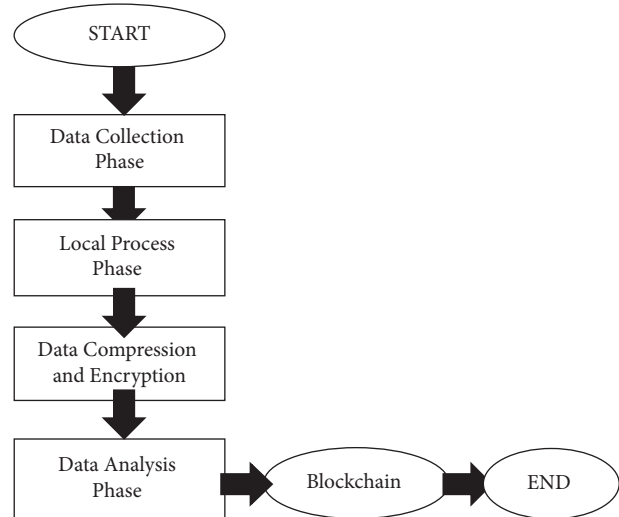


FIGURE 1: Flowchart of the proposed secure blockchain monitored scheme.

by the brain. In Figure 3, the hardware work of the proposed scheme has been shown.

3.1.2. Data Process Phase. In this phase, the Arduino kit plays as the brain for the proposed scheme where the sensor data are collected and processed [12–14]. To make it more intelligent, instead of sending the data directly to the cloud, either is it essential or not, the proposed scheme defined some condition to the process according to it, the processor decides to send or not. If the readings are equal to the usual case for the patient (each case is different from patient to other) so no need to send to the cloud. Otherwise, the local processor sends the data to the cloud. This scheme reduces the data sent to the cloud and sends only the crucial data.

3.1.3. Data Compression and Encryption Phase. This is the main contribution of the proposed scheme. In this phase, data are compressed and secured with the help of the transformation mechanism. The CS method is used for data compression and the encryption process to enhance the security and energy model for the proposed work. CS [13] is a new sampling theory in many applications. The CS method's power came from the truth that it can sample and compress in the same step rather than a sample and then compress as all other methods. The CS framework can be expressed as follows: If signal $X \in R1 \times N$ where this signal is sparse by its natural or by any transformer, i.e., X can be expressed as $X = \Psi g$, where $\Psi \in RN \times N$ is the transformer matrix, and g is the sparse representation of X , then the compressed sample of X can be obtained by

$$Y = \Phi X, \quad (1)$$

where $\Phi \in RM \times N$ is the CS matrix and M, N , and $Y \in R1 \times M$ is the compressed sample. Besides, CS can work as encryption [14] method, where X acts as the plain text, Y as the ciphertext, and Φ as the secret key. In the proposed scheme,



FIGURE 2: Representation of EEG sensor [11].

the local processor compress and encrypt the signal data using the CS matrix shared between the kit and the server. Thus, the proposed scheme is considered as energy and security-aware mechanism.

3.1.4. Data Analysis Phase. In this phase, the IoT cloud tool, like ThingSpeak server as used in the paper, receives the compressed data Y and then uses any CS reconstruction algorithms such as OMP, SP, etc. to reconstruct and decrypt the sensor data by solving

$$\begin{aligned} X &= \text{argmink}Xk1, \\ \text{Such that,} \\ Y &= \Phi X. \end{aligned} \quad (2)$$

Then, it analyses the data and sends it to the health centre or to any family member of the patient to help him in any emergency.

3.1.5. Consensus Mechanism. The proposed mechanism includes two types of miners: hospital miners and private or outsourced miners. The entities that of the hospital are termed here as Hospital Miners (HM) and also have Professional Miners (PM).

The hospital would generally not update the hardware frequently and carry little processing power to carry out the



FIGURE 3: The proposed scheme on hardware devices.

mining operation. It is generally used to minimize the cost of operations coupled with the scarcity of funds. Also, the hospital nodes are very optimally utilized and are seldom idle. These nodes shall contribute to the mining operation but without any incentive.

Further, individual hospital branches serve millions of patients data daily. On the contrary, individual branches like those in remote areas or towns or even individual rural branches have a relatively lesser load. Based on the patient data, classify HM as Heavily loaded HM (HHM) and lightly loaded HM (LHM). The next section proposes the leader election mechanism used to synchronize the mining of blocks with patient data to be verified.

3.1.6. Leader Election Algorithm. Each hospital has a patients data pool, in which all the verified patient's data are stored. The miners of each hospital store the patients' data into blockchain by composing these into the block. Block mining process needs to be synchronized to maintain the consistency of the blockchain. This responsibility is being handled by the leader election mechanism by synchronization of the mining process.

The leader miner is elected among several miners by the leader election mechanism for mining of each block. Each new block has mined the leader miner and is broadcasted to all the miners to achieve the consensus. The bootstrap server maintains the list of all active miners. The bootstrap server handles the allocation of slots for mining to the miners when patient data in any hospital branch; any miner of this hospital acts as leader miner mines the block during its timeslot while other miners participate in the consensus process.

3.1.7. Trust-Based Consensus Mechanism. Block is added to an active blockchain by the majority of blockchain applications requires 51% of polls. Involvement of real-time patient data processing, while developing an application is very challenging. The throughput and the system's response time reduces if all the nodes participate in the consensus mechanism. These issues are handled by proposing, a consensus mechanism based on the trust value and the miner's load. The proposed consensus mechanism reduces the time required to achieve consensus and the message exchange overhead. To achieve this objective, a policy that ensures only selected miners participate in the consensus process is implemented. Selection of these miners depends on their trust value.

The status table is being maintained by each miner comprising of the attributes such as CPU load, computational resources, node id, trust value, and CPU load status of other miners. Initially, the trust values are assigned to each miner as described in the next subsection. Later, the miners' trust value is updated based on each block's final consensus and the historical correctness of patient data carried out by miners.

3.1.8. Trust Value Estimation of Miners. Estimation of the trust value of miner is based on the three attributes. Once this trust value is estimated, required reliable miners can be selected based on the consensus mechanism.

(i) Response Time (RT) of each node along with its communication (bandwidth) time, (ii) Computation Resources (CR) available at each node, and (iii) Trustworthiness is based on the correctness of patient (CoPd) historical data, and its verification is performed while adding a new block.

Trust Value (TV) is computed as follows:

- (1) RT is set to 1, if the high bandwidth link connection is present, response time is expected to be faster. In absence or with a slower bandwidth connection RT is more, so it is set to 0.

- (2) If Computational Resource (CR), CR is set to 1, if Response Time (RT) is <30 milliseconds, else CR is set to 0, if Response Time (RT) is ≥ 60 milliseconds. Computational Resource (CR) is state of the art at any node. If RT lies between 30 and 60 milliseconds, it is set to 0.5.

- (3) When miner performs the correct verification of patients data, the value of CoPd is increased by 1. Otherwise, the value of CoPd is decreased by 5. Trust value is estimated as

$$TV = RT + CR + CoPd. \quad (3)$$

Trust value of the miners is broadcasted. The attribute table is maintained by each miner as follows:

- (A) Load of HM stored on the node. Nodes with load above a certain threshold are designated as heavily loaded hospital system miners (HHM), lightly loaded hospital system miners (LHM).
- (B) Further the same list is sorted based on the value of TV (Trust Value).
- (C) List of private miners is sorted based on TV score. TV of PM's above a certain threshold are designated as highly reliable or else are labelled trusted or suspicious.

Miners with threshold value ten and above are highly reliable miners, miners with threshold value between 5 and 10 are moderately reliable, suspicious miners have threshold value between 0 and 5, and traitor miner have threshold value less than 0. The miners are categorized into five different clusters in the proposed system based on their Trust Value (TV). The categorized five clusters are:

- (i) C1: highly reliable HHM
- (ii) C2: highly reliable LHM
- (iii) C3: highly reliable PMs
- (iv) C4: moderately reliable LHMs and PMs
- (v) C5: other miners or untrusted miners

C1, C2, and C3 include miners having a TV of 10 and cluster C4, the TV of miner lies in the range of 5–10. Cluster C5 contains miners whose TV is below 5. Miners having TV below 5 have fewer chances to be selected for participating in the consensus mechanism.

As soon as creating a new block takes place, this information is broadcasted to all HMs and PMs. For attaining consensus, only 25% polls with nodes in C1, 50% in C2, 25% in C3, and 25% polls in C4 are required in the proposed approach. These nodes participate in the consensus mechanism and perform the verification of new blocks since C3 carries state of the art computational resources deployed especially for a mining job. Hence, 25% of these participate in the consensus mechanism.

So, patient data that exist in this new block are verified by fewer nodes as compared to patient data verification by all nodes as done in PoW systems. The new block becomes part of blockchain based on the verification process's outcome,

and all the nodes are intimidated, if the majority vote is achieved. This proposed method saves network bandwidth and computation time by reducing the overhead of broadcasting by 50%.

3.1.9. The Leader in Consensus Mechanism. It is the leader's responsibility to mine the new blocks. Hence, consensus needs to be achieved on the new block. Once the block is created, the block's patient data must be verified before becoming part of the blockchain.

Multicasting is used in the proposed consensus mechanism instead of broadcasting. Based on the TV, the miners are selected to perform the verification new block. The leader miner does this task. Each node in the network maintains the status table. The leader randomly selects 25% miners from C1 cluster, 50% miners from C2 cluster, 25% miners from C3, and 25% of C4 as mentioned earlier.

Patient data are verified by the miners, selected for performing the verification known as consensus agents. The leader miner sends the new block for verification to these consensus agents. The consensus agent is also verifying the leader's digital signature. Once the consensus agent does the verification, the consensus is broadcasted in the network.

New block received from the leader is stored in a temporary buffer by all miners, including consensus agents. All the miners receive consensus polls. All this information is stored in a table maintained by a miner. Also, each consensus agent can identify from the table. The miners can update TV of the consensus agents based on trust management policies and polls.

Each miner creates a feedback table for each new block to store the consensus vote of the agents. Feedback table bifurcates the record in two parts. One part contains the list of agents in favour to add the block, and second part contains the agent list not in favour of adding the block, for every new block, the hash of the block, consensus agent's node id, cluster in which the agent belongs and the repose time is stored for both the favourable agents and the nonfavourable agents.

The arrangement for the real scenario has shown in Figure 4. For real setup, a scenario of the healthcare system has been considered. The main component of the setup is Arduino, Bluetooth, Cloud Server, and EEG sensor-enabled device, which collects the EEG data from the human body. The detail of the components are shown in Figure 2 are as follows.

4. Results, Discussion, and Analysis

This section of the paper gives details about the simulation setup and environment used in the experimental work of proposed method. And also, a comparative analysis is done between proposed method and other novel proposed solution in literature. In the process of comparative analysis, on certain parameters, proposed solution performance is better as compared to other proposed novel methods available in the method. Simulation setup and comparative analysis are explained below.

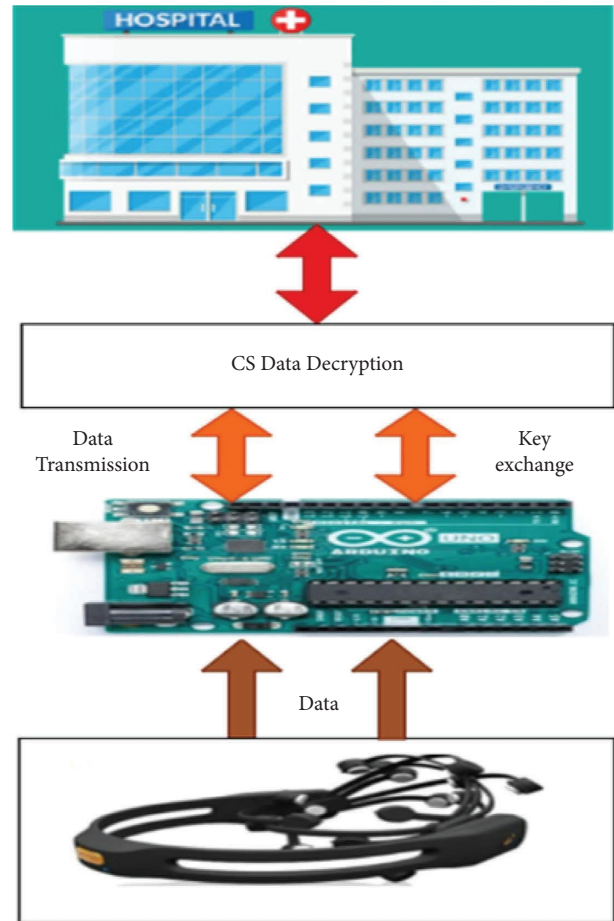


FIGURE 4: Proposed scheme example scenario.

4.1. Simulation Setup and Environment. In this section, the proposed technique has simulated using MATLAB R2016a. The entire experiments' implementation is on i7 intel core 7700HQ 2.80 GHz, 16 GB storage, and 1 TB hard disk. Figures 5(a) and 5(b) show the EEG signal in the time domain and DCT domain, respectively.

Figures 5(a) and 5(b) show that the collected EEG signal can be correctly reconstructed on both sides' cloud-side using the same CS matrix such that Figures 6(a) and 6(b) presents the reconstruction signal.

Figures 7(a) and 7(b) show that it is clear that the cloud-side cannot correctly reconstruct the EEG signal if it uses a different CS matrix, which explains the power of the CS method to protect the original data.

4.2. Comparative Analysis with State-of-the-Art Techniques.

In this section, the results include comparing different-different algorithms based on PRD value, execution time, and compression ratio. Percentage Root-mean-squared Difference (PRD) values for different existing algorithms is calculated at a different percentage of CR. In signal reconstruction, PRD value and execution time have a significant role in different-different CR values. Table 1 value of irls has better performance till 50 percent of CR value except for proposed algorithm (as proposed uses features of CS) but

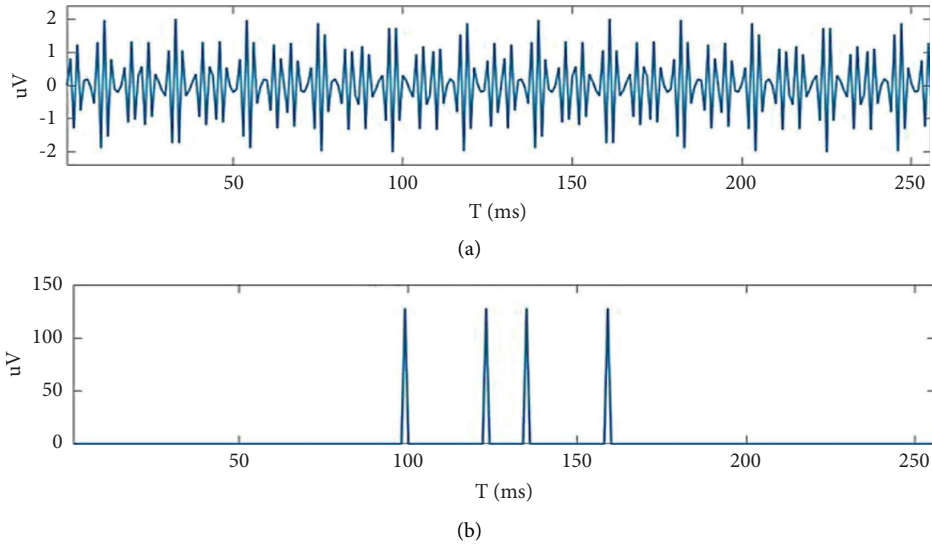


FIGURE 5: (a) Original EEG signal in time domain and DCT domain. (b) Sparse representation of EEG signal in time domain and DCT domain.

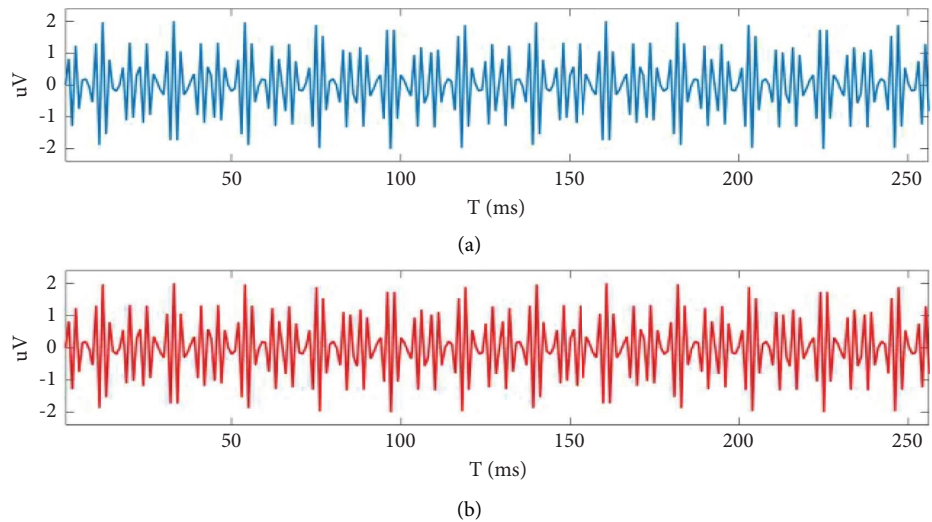


FIGURE 6: (a) Original EEG signal. (b) EEG signal reconstruction using correct CS matrix.

after that start declining, and considering the performance with respect to execution time, irls needs the most prolonged execution. As per as PRD or reconstruction is concerned, there are differences in performances in different ratios.

Table 1 contains the PRD values for various algorithms at different-different compression ratios. By the inspection of the table, irls' performance in terms of PRD is better from 10 percent to 50 but after that performance starts weakening. On the other hand, the proposed algorithm shows better or consistently better performance from the beginning till last. Figure 8 shows how the proposed algorithm has better performance or less PRD value than previously proposed algorithms at different-different compression ratios.

The proposed scheme is compared with [1, 2, 6, 7], and [8] scheme, the performance of the proposed scheme is better as per the parameters CR and PRD. According to

result from analysis proposed scheme in terms of compression ratio is 57.42%, 18.18%, 88.11%, 84.32% better concerning [1, 6, 7], and [8], respectively. Also in terms of PRD value the proposed scheme is 34.21%, 29.70%, 28.77%, 18.18%, 24.61% better with respect [1, 2, 7, 8], and [6], respectively. This paper presents a comparative analysis of CS for providing the EEG acquisition, compression, and security at the same time by utilizing the property of CS.

Table 2 BP outperforms the proposed algorithm and all other in term of execution time but also refers to Table 1, where BP algorithm is having high PRD value compared to the proposed algorithm. It signifies that the reconstruction of BP is poor as compare proposed one.

The proposed algorithm shows compromise in terms of the trade-off between the compression ratio and execution time, but same time outperforms in term of PRD

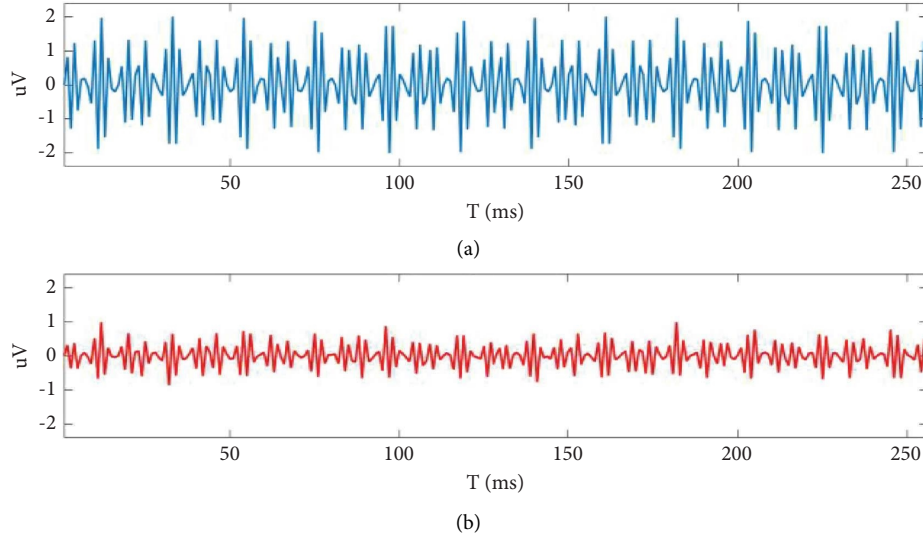


FIGURE 7: (a) Original EEG signal. (b) EEG signal reconstruction using incorrect CS matrix.

TABLE 1: PRD value for various compression ratio.

Algorithm	PRD value of various algorithms at different compression ratio								
	10%	20%	30%	40%	50%	60%	70%	80%	90%
CoSaMP	3.71833	4.38933	5.2569	6.43115	7.95982	10.71125	17.21511	55.38489	121.4902
BP	1.93039	3.34312	5.21037	7.99975	12.40657	20.39202	33.87659	56.92192	93.57194
SP	3.82239	4.42112	5.18738	6.24019	7.71914	10.08931	16.42685	50.77127	115.0552
Irls	1.67508	2.68763	3.80952	5.19156	7.31346	11.0418	22.10197	53.4094	95.22029
OMP	2.81908	4.07385	5.33478	6.65368	8.56955	11.16104	16.18991	60.75641	136.2308
Proposed	1.37052	2.19897	3.11688	4.24764	5.98374	9.0342	18.08343	43.6986	77.90751

PRD: percentage root-mean-squared difference. Irls: iteratively reweighted least squares. CoSaMP: compressive sampling matching pursuit. BP: basis pursuit. SP: subspace pursuit. OMP: the orthogonal matching pursuit.

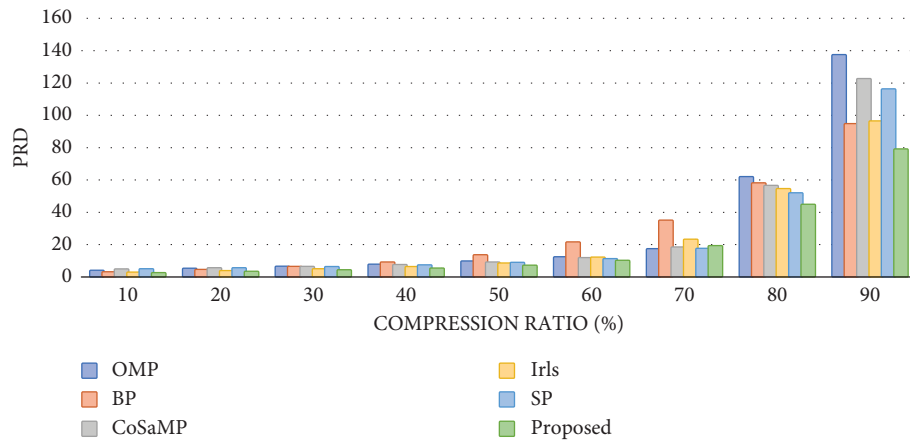


FIGURE 8: PRD value of various algorithms at different compression ratio.

value. The proposed algorithm has better performance because BP has a universally proportional relation with PRD and execution time. In other words, it concludes that BP has better execution time but wrong PRD value at 20 to 70 percent CR value. Figure 9 shows the execution time in second at a different-different compression ratio of various algorithms.

The proposed data-driven compression sensing can compress various types of physiological signals by using the data encoding scheme. CS only considers a few random samples, which are used to acquire signals. The measurements in CS does not learn from the previous measurements, i.e., they are nonadaptive. As a result, the generated compressive measurements are relatively less and transmitted or

TABLE 2: Execution time for various compression ratio.

Execution time in seconds of various algorithms at different compression ratio									
	90%	80%	70%	60%	50%	40%	30%	20%	10%
CoSaMP	9.03133	6.05869	3.9787	2.46576	1.22584	0.49566	0.21329	0.06644	0.01562
BP	0.22781	0.1892	0.15213	0.12661	0.10516	0.07744	0.0594	0.04697	0.03465
SP	4.92789	3.32618	1.83326	1.12332	0.57079	0.29381	0.12342	0.04422	0.01199
Irls	27.6428	20.0925	13.7849	9.59882	6.37131	3.89158	1.89596	0.82566	0.23672
OMP	25.8634	16.5028	10.4161	6.02514	3.19693	1.34673	0.46057	0.13816	0.02299
Proposed	4.03191	2.72142	1.49994	0.91908	0.46701	0.24039	0.10098	0.03618	0.00981

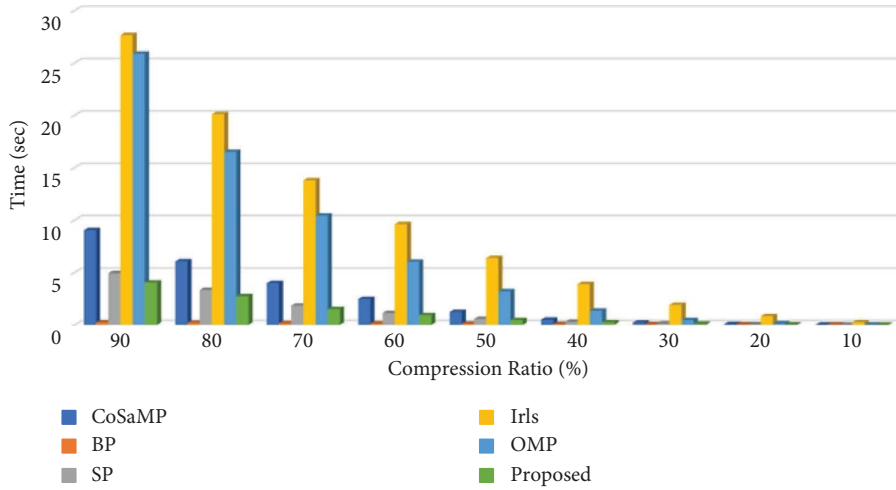


FIGURE 9: Execution time in seconds of various algorithms at different compression ratio.

TABLE 3: TME and MFC analysis in a varying number of nodes in the network.

S. No	N	c1	b1	c2	b2	c3	b3	c4	b4	TME	TFC
1	90	25	6.25	25	12.5	15	3.75	15	3.75	2336.25	934.5
2	180	45	11.25	45	22.5	45	11.25	45	11.25	10068.75	3356.25
3	270	65	16.25	65	32.5	95	23.75	55	13.75	23201.25	7935.5
4	360	95	23.75	115	57.5	95	23.75	75	18.75	44426.25	14449.75
5	450	115	28.75	145	72.5	125	31.25	95	23.75	70156.25	22674.5

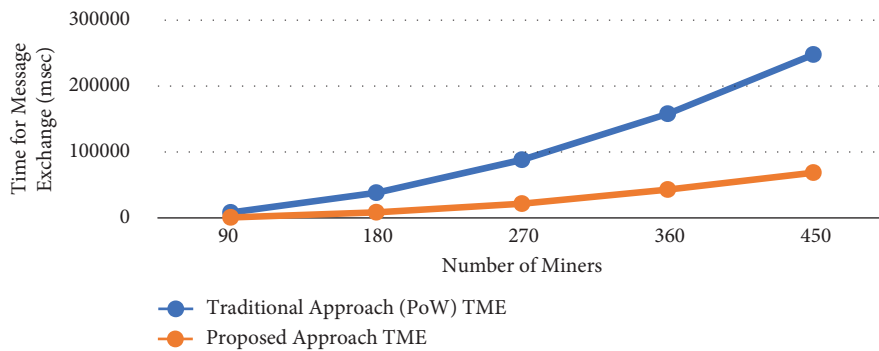


FIGURE 10: Time for message exchange (millisecond).

stored quite easily. So, here the signal is compressed while acquiring and is named as compression sensing. CS meets all the requirement of a resource-constrained WBAN and also provides lightweight security, Table 3.

The consensus for any new block is achieved in 24% less time than the proof-of-work (PoW) approach.

From Figure 10 and Table 4, it is clear that time for exchanging message is very less as compared to traditional

TABLE 4: TME and MFC comparison of the traditional and proposed approach.

S. No	N	Traditional approach (PoW)		Proposed approach		Message reduction in proposed approach (%)	
		TME	MFC	TME	MFC	TME	MFC
1	90	9890	4952	2336.25	934.5	23.6223458	18.8711632
2	180	39798	19902	10068.75	3356.25	25.2996382	16.863883
3	270	89698	44852	23201.25	7935.5	25.8659613	17.6926336
4	360	159598	79802	44426.25	14449.75	27.8363451	18.1070023
5	450	249498	124752	70156.25	22674.5	28.1189629	18.1756605

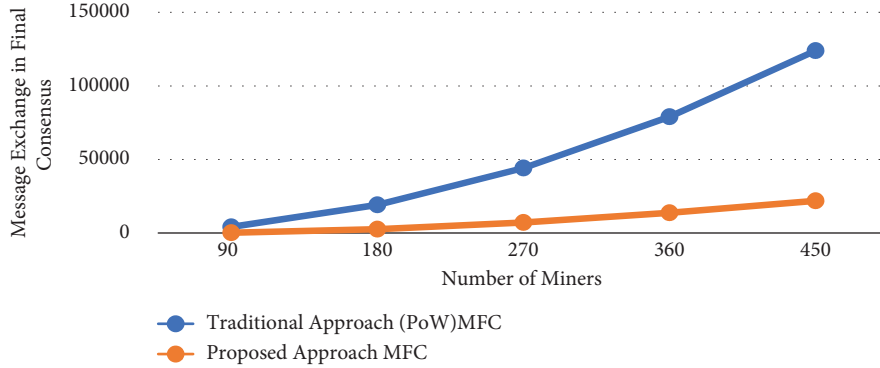


FIGURE 11: Message exchange in final consensus.

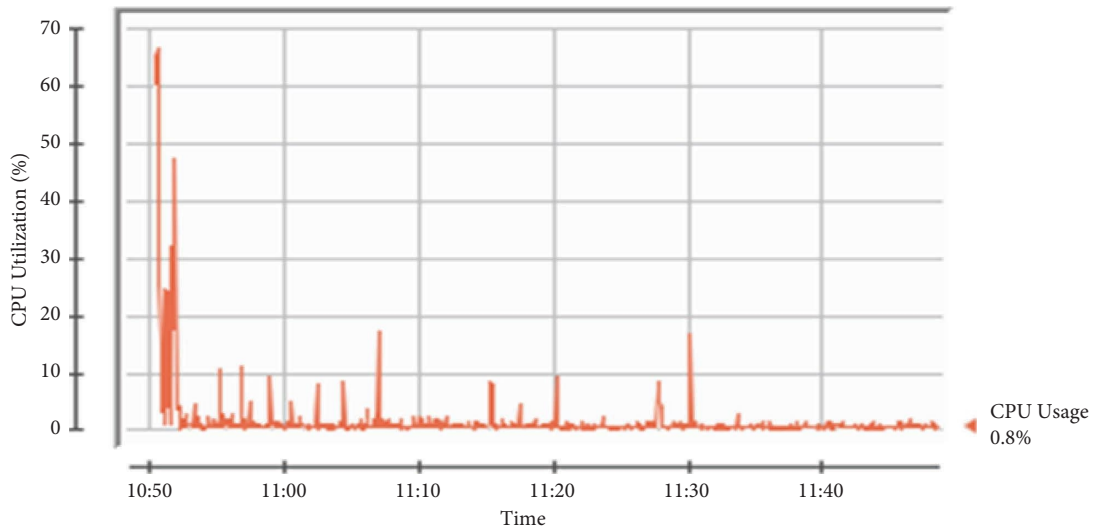


FIGURE 12: CPU utilization of miner process in an hour.

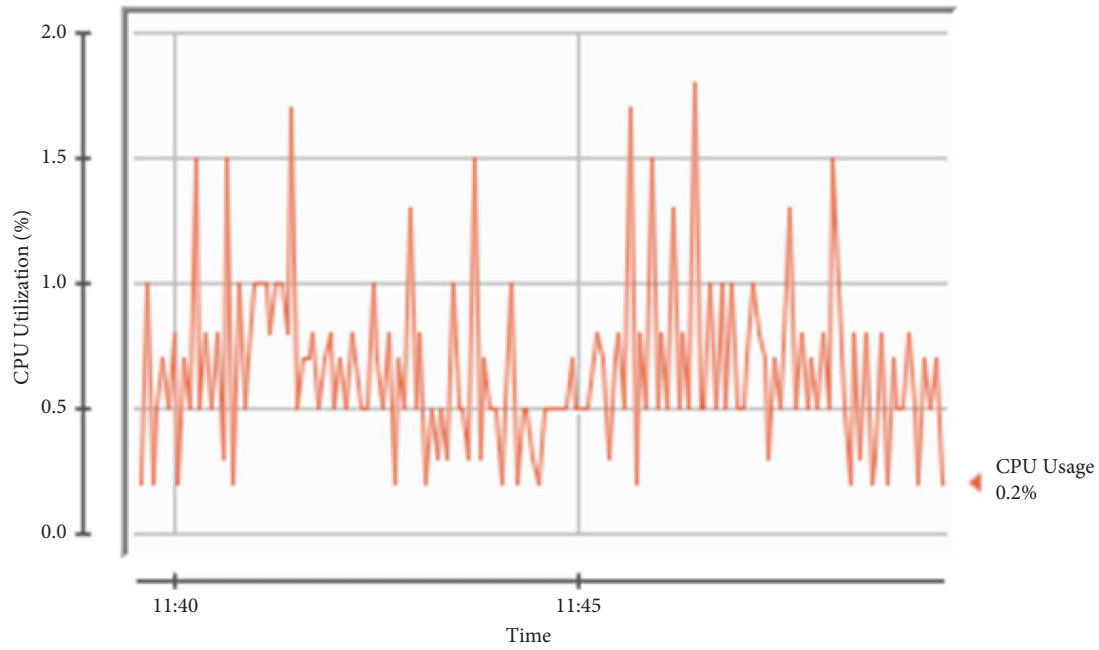


FIGURE 13: CPU utilization of miner process in 10 minutes time interval.

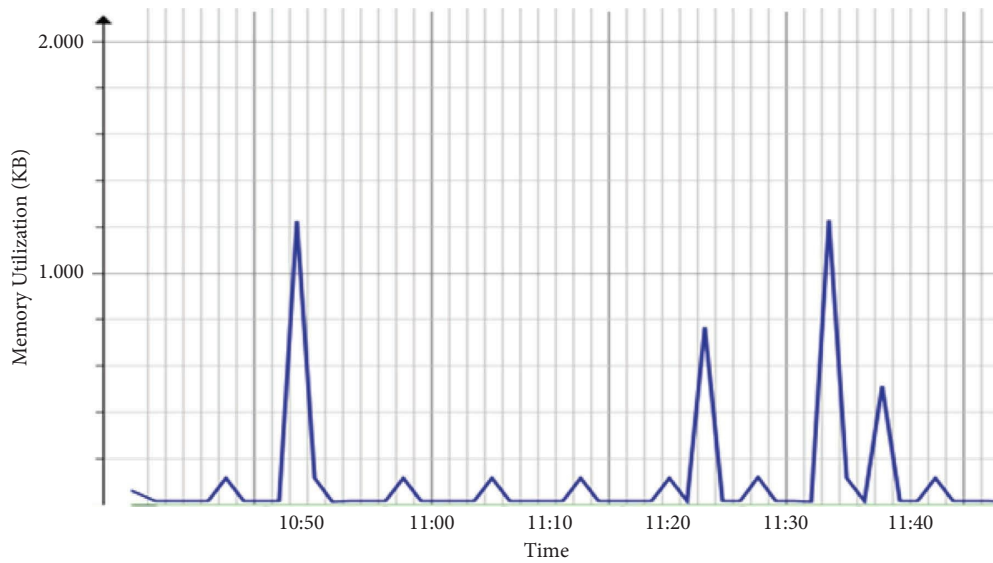


FIGURE 14: Memory utilization of miner process during one-hour simulation.

approach. For instance, if the number of minors are 180, then traditional approach is taking 50000 ms, while in proposed approach time is reduced to 1 by 10 times, i.e., 5000 ms. In final consensus, time ration is again reduced to 1 by 9 times. Figure 11 shows that when number of minors are 270 then traditional approach is taking 45000 ms while proposed approach is taking only 5000 ms.

The shallow CPU usage is required for leader election mechanism. In Figure 12, CPU utilization while experiment lies in the range of 0.9% and 14%. While simulating one-hour duration, as shown in Figure 13, the peak CPU utilization is 21%.

From Figure 14, the memory utilization peak value is 1180 KB, and the minimum value is under 16 KB. The

network utilization peak value is 11 KB per minute. The proposed consensus mechanism works well even with low configuration systems.

5. Conclusion

With the growth in need of modern/advanced health care communication system and application specifically designed for a disease such as Parkinson's, continuous monitoring of biosignal in real-time can play a key in day-to-day life. The advantage of continuous monitoring is that immediate response can send to the appropriate place whenever the patient gets an attack of the disease mentioned above. The patient's neurons signal is maintained consistently and update about the patient's health from the starting to end if any abnormality is noticed in the patient's EEG, then immediate action is taken to safeguard his life. The brain's physiological signal collection is processed by using the CS and transmitted through the proposed solution. Message exchange per consensus process is much lesser than the traditional proof-of-work (PoW) approach by using multicast instead of broadcast during consensus message exchange. Thus, the communication overhead is reduced. The consensus for any new block is achieved in 24% less time than the PoW approach. The shallow CPU usage is required for leader election mechanism. CPU utilization, while experiment, lies in the range of 0.9% and 14%. While simulating one-hour duration, the peak CPU utilization is 21%. The memory utilization peak value is 1180 KB, and the minimum value is under 16 KB. The network utilization peak value is 11 KB per minute. The proposed consensus mechanism works well even with low configuration systems.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

- [1] M. Memedi, G. Tshering, M. Fogelberg, I. Jusufi, E. Kolkowska, and G. Klein, "An interface for IoT: feeding back health-related data to Parkinson's disease patients," *Journal of Sensor and Actuator Networks*, vol. 7, no. 1, 14 pages, 2018.
- [2] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: a survey," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1658–1686, 2014.
- [3] A. K. Teshome, B. Kibret, and D. T. H. Lai, "A review of implant communication technology in WBAN: progress and challenges," *IEEE Reviews in Biomedical Engineering*, vol. 12, pp. 88–99, 2019.
- [4] S. Javadi and M. Razzaque, "Security and privacy in wireless body area networks for health care applications," *Signals and Communication Technology*, Springer, Berlin, Heidelberg, pp. 165–187, 2013.
- [5] S. Cohen, L. R. Bataille, and A. K. Martig, "Enabling breakthroughs in Parkinson's disease with wearable technologies and big data analytics," *mHealth*, vol. 2, no. 5, 20 pages, 2016.
- [6] B. Harrison and M. Guo, "Ontario health cut backs: overview and specific impact on primary care," *University of Ottawa Journal of Medicine*, vol. 5, no. 1, pp. 21–25, 2015.
- [7] Y. S. aldeen and K. Qureshi, "Solutions and recent challenges related to energy in wireless body area networks with integrated technologies: applications and perspectives," *Baghdad Science Journal*, vol. 17, no. 1, p. 0378, 2020.
- [8] Q. Kester, L. Nana, and A. C. Pasco, *A Novel Cryptographic Encryption Technique for Securing Digital Images in the Cloud Using AES and RGB Pixel Displacement*, European Modelling Symposium, Leipzig, Germany, 2013.
- [9] W. Diffie and M. E. Hellman, "Privacy and authentication: an introduction to cryptography," *Proceedings of the IEEE*, vol. 67, no. 3, pp. 397–427, 1979.
- [10] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for health care applications," *Egyptian Informatics Journal*, vol. 18, no. 2, pp. 113–122, 2017.
- [11] V. Kumar, N. Badal, and R. Mishra, "Body sensor networks architecture and security issues in healthcare application," *IOP Conference Series: Materials Science and Engineering*, vol. 1022, pp. 012075–12112, 2021.
- [12] V. Sharma, S. Kumar, and S. Bhushan, "An overview of data redundancy reduction schemes in WSNs," in *Proceedings of the 2017 3rd International Conference on Advances in Computing, Communication and Automation (ICACCA)(Fall)*, pp. 1–8, IEEE, Dehradun, India, September 2017.
- [13] S. Chauhan and S. B. Tyagi, "Performance evaluation of reactive routing protocols in VANET," *International Journal of Innovations and Advancement in Computer Science*, vol. 3, no. 9, pp. 189–193, 2014.
- [14] M. Diwakar, P. Singh, P. Kumar, K. Tiwari, and S. Bhushan, "A critical review on secure authentication in wireless network. Machine learning," *Advances in Computing, Renewable Energy and Communication*, pp. 623–633, Springer, Singapore, 2022.
- [15] K. Lorincz, D. Malan, T. Fulford-Jones et al., "Sensor networks for emergency response: challenges and opportunities," *IEEE Pervasive Computing*, vol. 3, no. 4, pp. 16–23, 2004.
- [16] M. Ghamari, B. Janko, R. Sherratt, W. Harwin, R. Piechocki, and C. Soltanpur, "A survey on wireless body area networks for eHealthcare systems in residential environments," *Sensors*, vol. 16, no. 6, p. 831, 2016.