Smart Wireless Sensor Technology for Healthcare Monitoring System using Cognitive Radio Networks

Tallat Jabeen , Ishrat Jabeen , Humaira Ashraf , Ata Ullah , N.Z Jhanjhi * , Rania M. Ghoniem , Sayan Kumar Ray

Posted Date: 2 June 2023

doi: 10.20944/preprints202306.0113.v1

Keywords: Smart Sensor; Sensing System; Wearable Sensor; Health Monitoring; Encryption

Article

Smart Wireless Sensor Technology for Healthcare Monitoring System using Cognitive Radio Networks

Tallat Jabeen [1], Ishrat Jabeen [2], Humaira Ashraf [3], Ata Ullah [4], N.Z Jhanjhi [5,*], Rania M. Ghoniem [6] and Sayan Kumar Ray [7]

[1] Faculty of Engineering and Information Technology, University of Technology Sydney UTS, Australia; tallat.jabeen@student.uts.edu.au
[2] School of Interdisciplinary Engineering & Sciences (SINES) NUST, Islamabad 44000, Pakistan; Ishrat.jabeen@sines.nust.edu.pk
[3] Department of Computer Science and Software Engineering, International Islamic University, Islamabad 44000, Pakistan; humaira.ashraf@iiu.edu.pk
[4] Department of Computer Science, National University of Modern Languages (NUML), Islamabad, Pakistan; aullah@numl.edu.pk
[5] School of Computer Science SCS Taylor's University, Subang Jaya 47500, Malaysia
[6] Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia; rmghoniem@pnu.edu.sa
[7] School of Computer Science SCS Taylor's University, Subang Jaya 47500, Malaysia; sayan.ray@taylors.edu.my
* Correspondence: noorzaman.jhanjhi@taylors.edu.my

Abstract: Programmable Object Interfaces are increasingly intriguing researchers because of their broader applications, especially in the medical field. In Wireless Body Area Network (WBAN), for example, the patients' health can be monitored using clinical nano sensors. Exchanging such sensitive data requires a high level of security and protection against attacks. To that end, the literature is rich with security schemes that include the advanced encryption standard, secure hashing algorithm, and digital signatures that aim to secure the data exchange. However, such schemes elevate the time complexity rendering the data transmission slower. Cognitive Radio technology with a medical body area network system involves communication links between WBAN gateways, server and nano sensors rendering the entire system vulnerable to security attacks. In this paper, a novel DNA-based encryption technique is proposed to secure medical data sharing between sensing devices and central repositories. It has less computational time throughout authentication, encryption, and decryption. Our analysis of experimental attack scenarios shows that our technique is better than its counterparts.

Keywords: smart sensor; sensing system; wearable sensor; health monitoring; encryption

1. Introduction

The Internet of Things (IoT) supports an ecosystem in which digital devices and computing sensors can establish human-to-human or human-to-computer interaction. Wearable computing Nano Sensors (NSs) are used in Wireless Body Area Networks (WBAN) to gather health-related data from the patient's body and transfer them to a biomedical server. This kind of communication demands high level of security measures to guard against intruder attacks [1]. The DNA Encryption Algorithm (DEA) [2] is one of the security measures that is adopted to protect data transmitted between nano sensors and the biomedical server through the Cognitive Radio Network (CRN) [4].

Authentication is another security challenge that needs to be tackled to protect the medical networks from untrusted users. [3]. The cognitive radio network (CRN) optimizes radio resource usage by exploiting the unused, yet authorized range, with an appropriate impedance moderation procedure. It first detects the idle spectrum from multiple base stations and then transmits data to

 doi:10.20944/preprints202306.0113.v1

the hospital's server via a gateway. Depending on their priority, primary and secondary users are granted access to this spectrum [4].

The real concern with the WBAN-CRN system is its vulnerability to security attacks and excessive power consumption, which may make the system unreliable. Attackers can manipulate data by fake injection and can cause interference by maliciously congesting the traffic.

In this work, we introduce a new encryption technique that is based on the DEA algorithm and uses ElGamal algorithm to generate the encryption key. The proposed scheme focuses on the IoT model's authentication of the patients and sensors using the CRN that exploits idle bandwidth to route data traffic.

Our contributions to this research work are as follows:

1) We propose a DNA-based encryption technique to secure medical data sharing between sensing devices and central repositories.
2) Our proposed technique combines a delicate encryption algorithm, namely the DNA-based Encryption Algorithm (DEA), with a good key-generator algorithm to secure the WBAN-generated data within the CRN.
3) Our proposed technique has less computational time throughout authentication, encryption, and decryption.
4) The authentication process and encrypted data ensure that only valid users gain access to the network system with our proposed technique.
5) Our analysis of experimental attack scenarios shows that our technique is better than its counterparts.

The remainder of the article is structured as follows. Section 2 reviews the current security techniques in the literature. Section 3 details our new approach. In Section 4, we present our evaluation and results and conclude the work in Section 5.

1.1. Literature Review

The wide spread of IoTs has reached numerous domains including healthcare. As a result of its expansion, people are more vulnerable to security and privacy breaches [3]. This article proposed a secure agenda based on low power and limited resources. The proposed system used AES-CTR mode to initialize a counter value, which was then incremented over a pseudo-random sequence using a variable named (IV) initial vector value. The size of the counter value for encryption depends upon encryption algorithms like AES-128 bits, this size is also 128 bits. It uses simple XOR operation as CTR mode used XOR operation. We also used a similar approach in our proposed work. The design involves the intra and inter WBAN [4] approaches. In the former approach, the sensors around the patient's body utilize personal server as a passage to transmit signal towards the next level. In the latter approach, the patient's basic healthcare information is recovered by interacting with the primary system via the web. Beyond WBAN, there is another vital basic phase when the medicinal condition database or biomedical server is set up. Because it is made up of incredibly basic materials, security and protection are the most important considerations. To validate the patients' information, many information security solutions are provided. To validate the information, it uses an elliptic bend cryptography (ECC) technique with a solid key management structure. To ensure the information's unwavering quality and security, the system used registration, verification, and key exchange procedures.

Different encryption and decoding strategies are proposed for the information security in the WBAN domain yet at the same time there is a risk of multiple attacks. The malicious node attack in IoT-enabled WBAN was identified and dealt with using the BAN trust strategy [3]. It is difficult for a sensor node to connect legitimately, but it is necessary to transmit data. To determine whether a node is trustworthy to communicate or not, check to see if it has ever interacted with another node. If it has, the recommendations it receives from others are critical in determining the trustworthiness of that unknown node. In [29], genetic-based algorithm for data security is used to protect from attacks. Multiple schemes are analyzed for data security. The comparison analysis of lightweight numerically encrypted data with the optimal protocol is the best system for data delivery overall.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 June 2023 doi:10.20944/preprints202306.0113.v1

There are two kinds of cognitive radio-based systems: three -tiered and centralized cognitive networks. The former approach comprises of intra, inter and beyond WBAN communication. Three systems are included in the Cognitive Radio system, inventory system, CR controller, and CR client. The inventory device preserves NS information and passes it to the CR controller. CR controllers control the power of CR clients. The Intra-based approach involves NSs placed in or above the body which interconnect with cognitive radio controller within range of two meters [4,5]. The CRN can be merged with IoT as CRIoT to solve the scarcity problem in IoT. In [6], a packet sharing, mechanism is presented for CRIoT to reduce the delay and the number of dropped packets. Our work also reduces the delay inherently due to CRIoT model. In [7], a trust aware packet routing mechanism is presented for social CRIoT. It used a game theoretic-based approach for trusted channel selection. Our work also ensure secure communication by presenting cryptography function for CRIoT which is also applicable for social scenarios. M. Shafiq et al. presented routing mechanisms that are based on location protocols, data-centric protocols, hierarchical protocols, mobility protocols, Protocols based on multipaths, protocols based on heterogeneity and protocols based on QoS [8]. Similarly, our work also adopts the CRN-based routing mechanism for better communication and less delays. Khalid et al. presented the half-duplex based routing mechanism for the CRIoT to improve the throughput [9].

In CRIoT, the consumer senses the bandwidth to recognize the presence of idle spectrum with any frequency or time domain [9]. Moreover, a simulator for the full-duplex radio networks over IoT in presented in [10] where packets are sent and received among the sensing devices. Primary customers share their data arrangement or possibly code book with the secondary transmitter in overlay. Consider a scenario where the information for medicine and hospital observation data begins from the facilitator. In this case, the two applications have side data on each other's messages; on a similar frequency band, the overlay CR sends the MWBAN information to two targets. The primary patient is the medicine transmitter whereas in-clinic knowledge is the secondary. The system architecture of WBAN over CRN intended to transfer a limited amount of sensed data towards the remote server through the closest base station of cognitive networks [11]. Figure 1 illustrates the Body Cog BNC is the main part which acts as a gateway between WBAN and CRN. It transmits data from sensors to the server. Data can be transmitted layer wise through CRN [12].

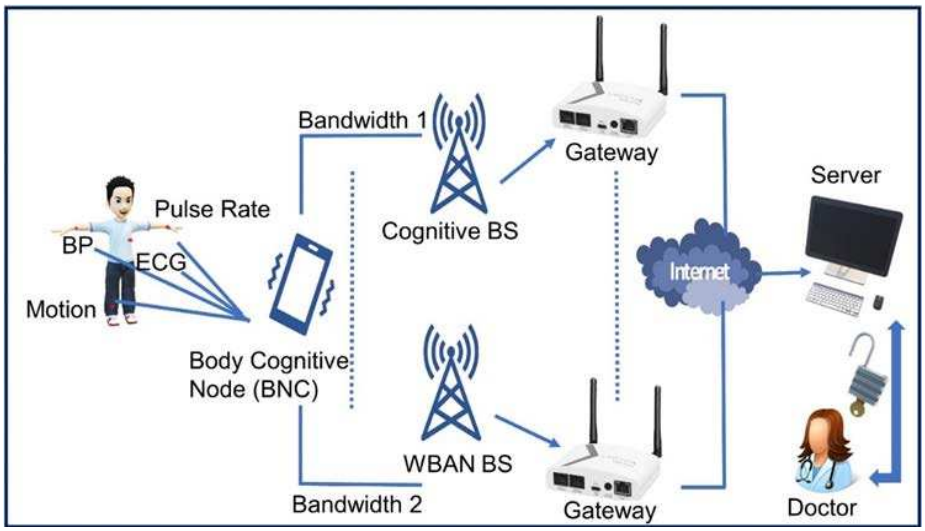

Figure 1. The WBAN-CR Network Architecture.

A CRN moderates the interference and enhances the effectiveness of the limited spectrum usage. In order to priorities the access of frequency channel, there are two types of users primary and secondary users. Primary users favored as compared to secondary because of real time and crucial data transmissions and they have higher priority to choose the available bandwidth. Spectrum sensing now requires sensing the idle bandwidth information to route the data, and the next step is

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 June 2023 doi:10.20944/preprints202306.0113.v1

to access the bandwidth. Bandwidths access functions coordinate to sense the idle spectrum and update the WBAN's channel access time. The amount of radio spectrum required for applications like mobile telephony, digital video broadcasting (DVB), wireless local area networks (Wi-Fi), wireless sensor networks (ZigBee), and the Internet of things [14–16] is immense and continues to rise. By 2021, nearly 50 billion cellular devices will be linked, necessitating a significant amount of spectrum [17]. The CR- based paradigm is explored for routing mechanism in [18] whereas the contention window-based mechanism is explored in [19]. In [20], a channel hoping mechanism is designed where secondary user can avail the network without clock synchronization at global level. It improves throughput and average time. The main benefit is that it provides wireless devices with opportunistic access to more bandwidth, allowing them to boost their achieved throughput [21]. Intrusion detection is the method of detecting harmful or illegal computer or network activities in CRNs [22]. Better use of existing spectrum resources has been accomplished with the aid of CRNs [23] by leveraging underutilized licensed spectrum [24,25]. For automation applications based on wireless communication, cognitive radio considerably reduces spectrum scarcity [26]. Secondary users (SU) in mobile cognitive ad hoc networks regularly detect the behavior of main users (PU) and opportunistically utilize PU's idle licensed channels [27]. It is critical to develop viable techniques to deal with interference and make efficient use of temporarily accessible frequency bands in order to maintain a high degree of communication quality [28,29]. It is also observed that various related schemes in the literature give high computational complexities in terms of deployment. This complexities enhances the cost of the whole system which is difficult to maintain the structure. The best resource distribution for cooperative CRN with opportunistic licensed spectrum access is examined. CRN is used as protocol to forward encrypted data towards server. Therefore, CRN is an optimal and cost effective selection as a protocol for data delivery.

Table 1 presents a comparison analysis of multiple related schemes with the proposed scheme based on some security attacks parameters. Literature related security technique had some stumbling blocks with attacks, but proposed security scheme provides all the safety parameters mentioned in the Table 1. Some of the solutions described in the related articles provide protection against attacks denoted by the rightly rectified symbol. Therefore, it is observed that proposed DNA based scheme with authentication process is lightweight and efficient in terms of security parameters and time complexity. Ismail et al. [35] and Zhao et al. [37] provide DNA based techniques to secure data over the networks. Technology, commerce, and social conventions have all seen rapid advancements in the twenty-first century [38]. Comparison analysis with the proposed scheme and the literature scheme is provided in the Section 5.

Table 1. Comparison of Security Analysis.

Research Schemes	Plaintext Attack	Eavesdropping Attack	Tempering Attack	Jamming Attack	Collision Attack	Sybil Attack	Selective Forwarding Attack
[30]	×	✓	×	✓	×	×	✓
[32]	×	×	×	✓	×	×	✓
[33]	×	✓	×	×	×	×	×
[34]	×	✓	×	×	×	×	×
Proposed work	✓	✓	✓	✓	✓	✓	✓

2. Materials and Methods

The architecture of our WBAN-CRN system comprises the DNA-based Security Encoding Algorithm (DEA) along with CRN protocol to encrypt data and authenticate patients and devices. The DEA is used to encode the data collected by the IoT-enabled WBAN system and the ElGamal's

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 June 2023 doi:10.20944/preprints202306.0113.v1

algorithm is used to generate the encryption key. The ciphertext is then transmitted wirelessly to the biomedical server through the CRN routing. The WBAN consists of nano sensor nodes attached to the patient's body to monitor and collect vital health data such as the body temperature, sugar level, heart beats (ECG), blood pressure, etc. This data is routed over the network through the CRN. It is used with multiple electromagnetic spectrums to transfer data to the server. It detects the idle spectrum and updates the WBAN channel sensing. Transmission of data and allocation of idle spectrum is also observed in the cognitive network. Figure 1 presents the architecture of the WBAN-CR network which consists of four components: sensors BNC node, access points, gateways, and the medical server that is easily accessible to the physicians. Each transmission between these components consumes less time and less computational resources.

The first line of defense against impersonation is to authenticate patients and the sensor devices attached to them.

The patients use their unique ID's associated with cellular phones to register with nano-sensors that use the device IDs to register with gateway. The nano sensors collect data and transmit them to the gateway for routing. In the sensor registration phase, nano sensors share unique identity SID for registration in the gateway's database.

The proposed DNA Encryption Algorithm (DEA) demands lesser computational time and memory space. First, an encryption key is generated using ElGamal's algorithm, and this key is subsequently used to encrypt data using the DEA algorithm. A symmetric encryption algorithm uses one key to encrypt and decrypt data, while an asymmetric algorithm uses a private key to encrypt data and a public key to decrypt them. The proposed scheme uses the ElGamal algorithm to produce a symmetric key to generate a mutual password for data sharing. First, two common prime numbers, P and D, decided by the parties who wish to establish communication. Then T is used to generate the ciphertext where T = (E)^d mod P, and E is a selected value.

Figure 2 elucidates our encryption scheme. In the decryption phase, the ciphertext is converted into binary from DNA table which is DNA sequence. The obtained data are used to recover values from S-box to apply circular left shift one. Now make four bits of two subsets each and take the first half of four bits to perform operation and ignore the second half of four bits as they were extended from the DNA.

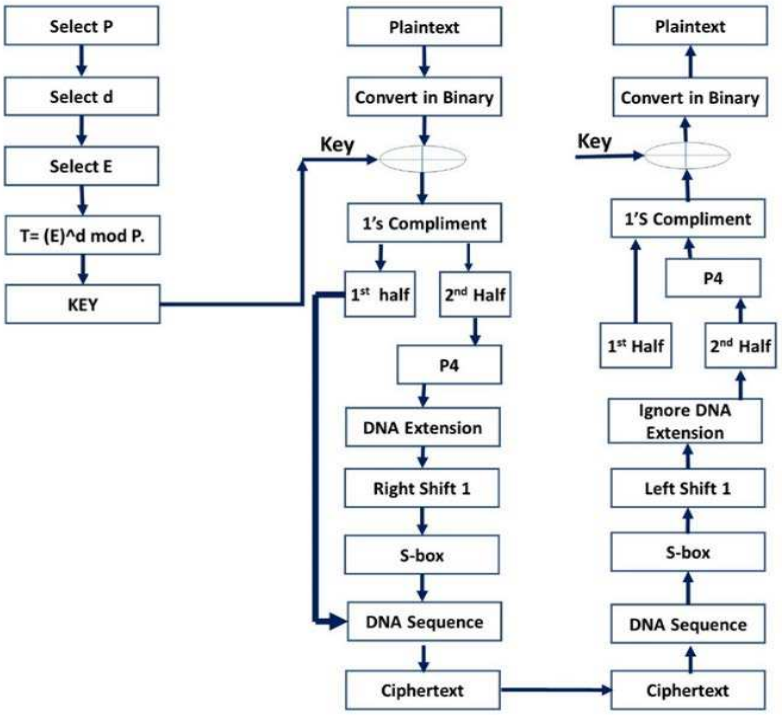

Figure 2. Encryption and Decryption Algorithm.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 June 2023 doi:10.20944/preprints202306.0113.v1

Then apply P4 substitution on the first half of four bits which combine the previous bits to make eight bits. Now take one's compliment and perform XOR operation with the key generated by the ElGamal algorithm.

The resulted binary data is eventually presented and displayed to the patient in decimal format (e.g., ECG data). to the patient. P4 is used to swap four bits' binaries with each other on the corresponding value in the table. This operation is performed on the second half of the encryption algorithm bits. There are four indices 1, 2, 3 and 4 to replace the corresponding indices. For example, 1 is replaced by 4, 2 is replaced by 1, 3 is replaced by 2 and lastly 4 is replaced by the 3rd value. S-box describes working of the proposed algorithm in steps and these steps are discussed deeply. Simple S-box contains binary values which are substituting in the encryption algorithm on demand and used while decrypting the data. Simple S-box contains row of 0,1 and column of 0,1. 00 in the box results into 1 and 01 gives 0, likewise 10 resulted to 1 and 11 gives 0. DNA standard contains binary values of two bits each and corresponding DNA sequence. There are four rows of 11, 01, 10 and 00 with their corresponding DNA sequences, 11 comprise the sequence 'G', 01 contains 'A', likewise 10 have sequence of 'T' and lastly 00 provides DNA sequence of 'C'. In encryption algorithm, first binary values are used to extend the bits. Next, perform AND operation of first row 11 with third 10 and second 01 with fourth 00, obtained group of four bits is used in encryption for further action. At last, binary value used DNA sequence to convert into Cipher text.

NS detects WBAN's data and gives information to personal device (PD) that sends data over idle bandwidth spectrum, which is then linked to BS. If PD receive data from the NSs securely then idle spectrum is sensed for the transmission of data. If PD does not get encrypted data from the NS, then idle spectrum of bandwidth is not sensed. Data is sent towards BS of cognitive networks successfully if it gets data from PD as illustrated in steps (2) to (13). BS transfers data towards gateway securely encrypted using DEA. If BS receive data from bandwidth securely then gateway transfer through clouds. If BS is not receiving data from bandwidth securely then gateway does not transfer any data for further actions. But if data is sent from BS to gateway successfully data is transferred towards medical server as demonstrated in step (18) to (31).

Algorithm 1: Key Generation and DNA Encryption

Key Generation

1. ***Begin***
2. *Select Prime number P.*
3. *Select Private Key D.*
4. *Select Public Key E.*
5. *T= (E)^d mod P.*
6. *Value of T will be key value*
7. ***End***

DNA based Encryption (at WBAN's Sensors)

8. ***Begin***
9. ***for** each NS ∈ PD **do***
10. *Sensor node sends authenticated data towards PD through DNA Encryption securely*
11. *Then idle spectrum is being sensed to transfer data*
12. *Through idle bandwidth spectrum PD transfer data to BS*
13. ***end for***
14. ***for** each NS ∈ PD **do***
15. ***if** (PD receives data from NS securely) **then***
16. *encrypted data is ready to transfer over idle bandwidth spectrum*
17. ***else if** (PD does not receive data in given slot from NS) **then***

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 June 2023 doi:10.20944/preprints202306.0113.v1

18. Bandwidth is not sensed for idle spectrum

19 else if** (BS receives data from PD successfully) **then

20 data is transferred to cognitive networks BS

21 end if

22 end for

DNA Encryption Algorithm (DEA) (at Cognitive networks)

Begin

23 BS transmits data to gateway safely encrypted using DEA

24 Data is transferred from the gateway to the medical server.

25 Data is detected by medical servers for further action.

26 end for each BS GW do twenty-first for twenty-first for twenty-first for twenty-first for twenty-first for twenty-first for twenty

27 If (BS safely receives data from the spectrum), then

28 Gateway is used to transport data over clouds.

28 Data is not identified by the Gateway to send over clouds if (BS does not receive data from any spectrum in specified slot).

30 If (data from BS to Gateway) is true, then

31 Gateway clouds deliver data to the medical server.

32 End if

33 End for

2.1. Mathematical Modelling

In $Y = x \oplus k$, Y is provisional text which is updating according to operations. Plaintext X calculates XOR with key k. Next, $Y1 = Yc$ where $Yc = YC1.YC2$. In equation, Yc is calculating one's complement of the short term generated cipher which is equal to Y1. Next, Yc is divided into two halves, denoted by YC1 and YC2. In case of $Yc = YC2 \rightarrow P4$, P4 is applied over the second half of the complement YC2 of four bits. P4 is the permutation which substitute bits accordingly. $Y2 = P4 \sim TDNA$ and $Y3 = \gg Y2$. Now four bits of permutation P4 need to extend into the eight bits with the help of DNA table which is equal to Y2. Then eight bits converted Y2 is circulated one shift right which creates temporary cipher of Y3. In $Y4 = Y3 \rightarrow S - box$ and $Y5 = YC1\ U\ Y4$. S-box is applied over the right shifted bits of Y3 which again convert eight bits into four bits and this short-term cipher is equal to Y4. Now, associate previously first half of the complement YC1 with Y4 to convert into eight bits again which generates cipher of Y5 i.e., $Y5 = DNAsq$ and $Z = Y5$. Apply DNA sequence on Y5 from DNA table which is equal to Z and it is actual generated ciphertext.

2.2. Cognitive Radio Network Protocol

The sender node selects 'A = (1-n, n = prime number)' and the receiver node selects 'B = (1-n, n = prime number)' The sender node selects three random numbers, 'P' and 'D and E, and then calculates the value of T that will be used to generate the key. The sender node calculates the T value from the $T = (E)\text{^}d\ MOD$ P formula, which is the key that is used for encryption. The sender node chooses plaintext to be sent to the sender node, instead of converting the plaintext to a binary value. If the key is generated, then the sender node uses the generated key and the binary value of the XOR key. One's complement of temporary cipher text is taken. Then generated text is divided into 2 subsets, and then leave subset1 as it is and perform operation on subset2. Apply Parameter four(P4) on subset 2. Now Extend the four bits from DNA extension to make 8 bit of data. Apply circular right shift 1 on 8 bits. Substitute values form S-box which make again 4 bit data. Now add subset 1 with the generated 4 bits data to make it 8 bits of data. Sender replaces the DNA sequence from the DNA table that is

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 June 2023 doi:10.20944/preprints202306.0113.v1

actually the ciphertext received. ELSE (if the key is not produced, then the key is first generated, then repeated) Sender node to submit encrypted text and Sender node ID to the Bandwidth sender node. After receiving the encrypted text from the receiver node, it then redoes all the operation in the backward place.

Figure 3 demonstrate that Steps (1)–(6) explore that WBNS's sensor generated plaintext is transferred to the server through cognitive network. Plaintext of WBAN is converted into 8-bits binary. The 8-bit binary values of step 2 are then XORed with the same bit of key generated by the ElGamal key generation algorithm. Then take one's compliment of the of the resulted binary data generated in step 3. Next, divide the generated 8-bit binaries into two halves. In Steps (7)–(12), initially it leaves the first half as it is and consider second half of the data. Apply parameter 4 (P4) on second half which generates 4 bits of data with their corresponding indexes.

Next, extend 4 bits of step 7 into 8 its by putting DNA values, perform AND operation on first value with third and second with four from DNA. After that, perform circular right shift one on 8-bit generated data of step 8. Substitute corresponding bits from S-box which convert binary data into 4 bits again. Next, add previously leaved bits of first half in step 6 which make 8-bit binary data. Finally, substitute 8-bit binary data into DNA sequence given in DNA table. Step 13 shows DNA sequence for ciphertext of the WBAN data.

The receiver receives encrypted data which is not readable at step (28). First, Substitute DNA sequence of the ciphertext with their corresponding binaries. Apply S-box on the generated values of step 2. Perform circular left shift one on the 8-bits data. 8 bits data is divided into two halves which makes two subsets of 4 bits. Ignore the second half of the bits in step 5 as they are DNA extended bits. Now apply parameter 4 (P4) on the first half and combine these bits with previously assigned bits which makes 8 bits of data. Take one's compliment of the resulted 8-bit data. Now perform XORed operation with the ElGamal key generation algorithm. The value is then translated into ASCII decimal places after all the decryptions. The SDEA is a secure algorithm with minimal computation time, good response, and difficult for attacker to intercept plaintexts.

For the duration of the enhanced network, the deployed sensor node needs judicious use of energy sources. The forwarder node relays information from all sensor nodes to the sink. Sensor nodes choose a path to the sink node that is idle and consumes less energy. The proposed work centered on determining the best data transmission path and lightweight security algorithm enhance its performance efficiency. The proposed energy-aware routing protocol lowers the overall network implementation cost as well as the amount of energy used by the network and sensors.

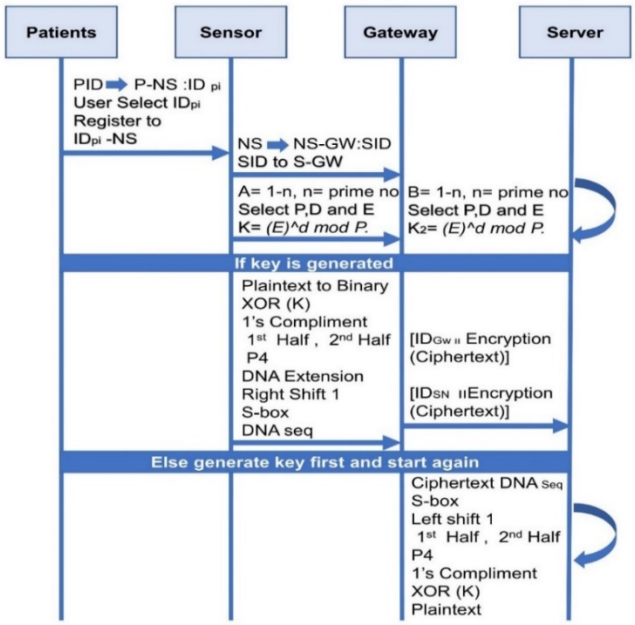

Figure 3. Secured Routing Protocol in a Cognitive Radio Network.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 June 2023 doi:10.20944/preprints202306.0113.v1

3. Security Analysis

Security analysis is mandatory to secure the data from different attacks. Network routing data may be compromised by attacker and data transmission must be secure.

3.1. Plaintext Attack

After obtaining the plaintext and the ciphertext, the attacker may attempt to analyze the relationship between plaintext and ciphertext. In cryptography, this is an attack that is very basic. The attack scenario when the user sends the data for encryption, encapsulating the piece of plaintext by the attacker, as shown in Figure 4. This known piece of data attacker attempts to recover the encryption algorithm that is then used as $P(C(S,R) = Z(P,C)$ for the decryption process, where P is plaintext that transmits data with a ciphertext pair from A to B, and Z is the attacker that attempts to recover data with known plaintext. Our introduced work prevents plaintext attack as the users do not send simple plaintext over the network. A known plaintext attack necessitates the recovery and analysis of a matched plaintext and ciphertext pair. The purpose is to determine which key was used. If you recover the key, you can decode other ciphertexts encrypted with the same key. Plaintexts always use the El Gamal's key generator that uses randomly chosen parameters, which are not possible for the attackers to discover.

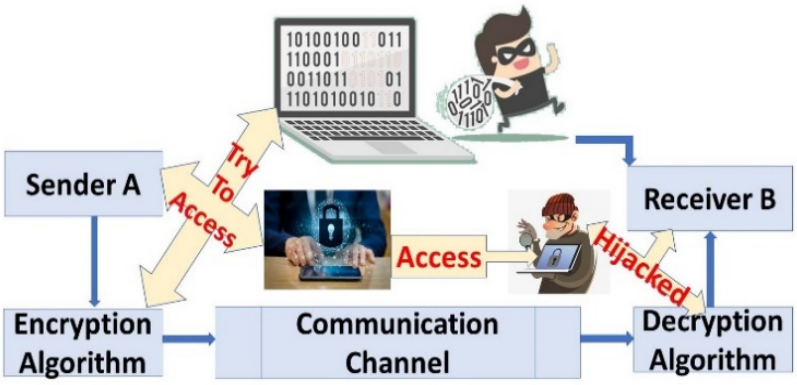

Figure 4. Plaintext Attack.

3.2. Eavesdropping Attack

A three-personal scheme, including a, sender, receiver and the man-in-middle (the attacker) is the proposed system. The smooth transmission channel is often disrupted by man-in-middle and the conversation between sender A and receiver B is secretly listened to by intruder Z as $E(A,B) = Z(E(A,B)) + Z(Ei+1(A,B))$, where E is encrypted data and $Ei+1$ shows addition of spoofed packet in encrypted data flow. The interaction is eventually manipulated. Due to the DEA algorithm and the authentication method, this scenario could be evaded in the proposed framework. The authentication process prevents third parties from intercepting the conversation.

3.3. Tempering Attack

Tempering is a sort of attack in which an attacker gains physical access to a node or obtains sensitive data on the node, such as cryptographic secret keys or other confidential data. The invader, who could change the system, then constrains it, or communication is substituted. Outsider Z gains physical access to data flow by breaking communication between nodes A and B.

$$(NA, NB) = (Z(NA)), (Z(NB)).$$

3.4. Jamming Attack

Jamming is an attack which interfere with the frequencies of the radio that the nodes of a system are using in jamming. It is the subset of denial of service (DoS) attacks. Data transmission path

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 June 2023 doi:10.20944/preprints202306.0113.v1

between sender and receiver dropped because of jamming attack. Intruder constructs an alternative communication path with receiver as presented in Figure 5. Data transmission path between sender S to receiver R is dropped and the jamming attacker Z links new path to transmits dummy data packets towards receiver R as $(\mathrm{NS}, \mathrm{NR}) = (\mathrm{NS}), (\mathrm{Z}\,(\mathrm{NR}))$. The suggested technique prevents this attack due of CRN. A cognitive network uses a priority-based and idle bandwidth spectrum for data transfer. The data transmission path is not obstructed by this idea. Data collision has also been prevented thanks to the adaptation of the idle spectrum.

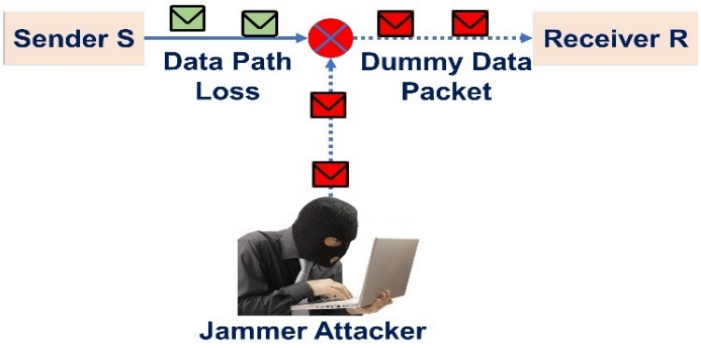

Figure 5. Jamming Attack.

3.5. Sybil Attack

Sybil attack is a type of attack that obstructs routing protocol using false identities. Data transmission between original node and authenticated node is disrupted by the Sybil nods that are using their multiple fake identities to creates hinders for communication. The Proposed technique avoided the Sybil attack by using authentication of involved nodes and other stockholders in the networks. Therefore, unauthenticated Sybil nodes are not considered part of the system and transmission remains smooth. It involves rounds of communication between original and authenticated nodes with the Sybil barriers. In the expression, $(NO, NA) = (NO), (NS\,(NA))$, NO is message originated node that transmits data towards NA node and NS shows the Sybil attacker that effects the smooth data transmission.

3.6. Collision Attack

When more than one node tries to forward data then collision of data occurs. In this situation, an attacker may intentionally cause collision to discard the transmitted data. It provides the concept of data collision by sending fake data by attacker Z to hit original data packet. I the expression, $(NS, NR) = ((NS) \times (Z))\,(NR)$, NS is sender node and NR represents receiver. The recommended technique prevented this attack by using authentication and cognitive radio protocol as shown in Figure 6.

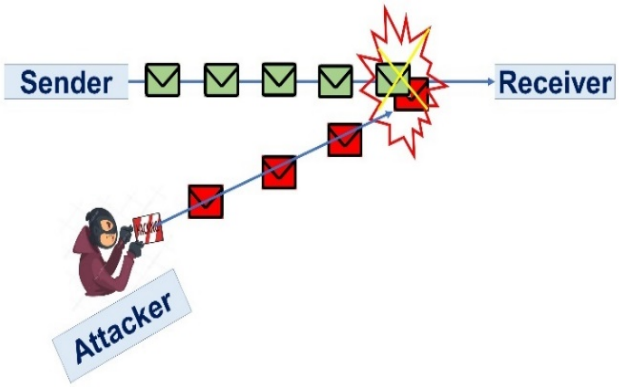

Figure 6. Collision Attack.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 June 2023 doi:10.20944/preprints202306.0113.v1

4. Results and Analysis

In our experiments, we used the MATLAB 2013a to simulate the cognitive radio networks. The field space of the simulation is 100 x 100 meters. The body sensors collect ECG data. WBAN detects the ECG of the human heart and give data results in detail. CRN used as routing protocol to transfer the WBAN's data to the biomedical server using bandwidth spectrum. The CRNs sense idle spectrum in multiple antennas by using an improved energy detector. This simulation gives detailed results of the proposed system. There are two types of evaluation measures performance evaluation and results evaluation. Performance evaluation contains time taken by the algorithm to encrypt or decrypt the data. We compared the computational time which is the time calculated by the algorithm to complete a specific task in limited time slot. The base schemes, AES-CTR [3] and ECC [30], are compared with ours.

4.1. Analysis of Authentication Time Complexity

Computational time interval of sensors authentication with patients and gateways is observed. It is noted that as the number of tiny sensors increased to register the response time also increase e.g., when sensor1 is registering the time taken is 0.5 and the 5 sensors take 3 seconds approx., As seen in Figure 7, overall time taken to authenticate the people is slower and efficient.

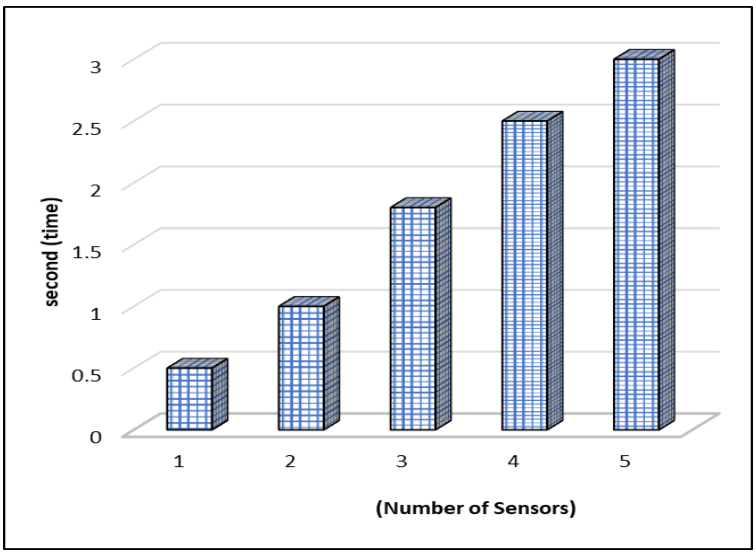

Figure 7. Time Complexity of Authentication Process.

4.2. Time Complexity for ElGamal Key Generation

The computational time is the time it takes the ElGamal technique to produce a key. The data bytes and time taken by the method to create the key for the encryption procedure are shown in Figure 8. The time used by the procedure increases as the number of data bytes increases. For 30 bytes, it takes 9.5 seconds, whereas for 60 bytes it takes 21 seconds to compute the data bytes for key production.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 June 2023 doi:10.20944/preprints202306.0113.v1

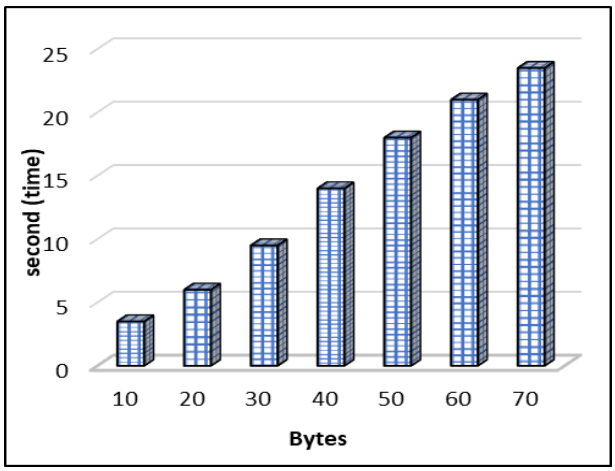

Figure 8. Time Complexity for ElGamal Key Generation.

4.3. Time Complexity Comparison for Key Algorithms

ElGamal key generation algorithm is used to support proposed encryption scheme and its comparison analysis is performed with the Diffie-Hellman Key generation method [30]. It is observed in Figure 9 that as the data bytes increased time taken is also increased e.g., 1 data byte took 2 seconds approx. in ElGamal method and deffie-hellman increased to 5 seconds at same amount of data byte. Analysis of time complexity of ECC techniques is presented in [31].

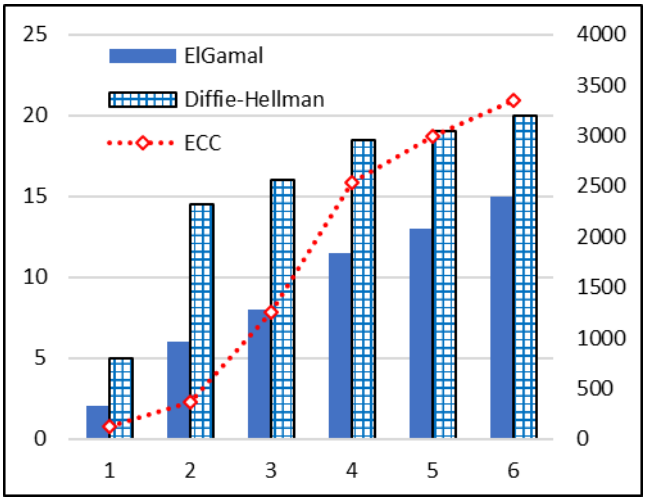

Figure 9. Time Complexity Comparison for Key Generation.

4.4. Time Complexity for Encryption and Decryption Algorithm

Plaintext conversion into ciphertext is known as encryption, and encryption time is the time taken by the algorithm to transform plaintext into ciphertext. The time taken by the proposed DEA is estimated. Figure 10 illustrates that time also increases as the data bytes for encryption increase. The proposed DEA takes less time with even larger data bytes of encryption as it is an efficient algorithm. It is noted that as the data bytes increasing time of encryption algorithm also increasing gradually time at 10 data bytes is 2 seconds while at 30 data bytes it is almost 7 seconds. Decryption is the process of fetching plaintext from the ciphertext, and the time taken by an algorithm to fetch the original data is known as decryption time. Figure 10 also shows that various byte of data takes different time to decrypt the data. Decryption time at 10 data bytes is 0.5 seconds and at 20 data bytes it is 2.5 approx. Time is varying according to data bytes.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 June 2023 doi:10.20944/preprints202306.0113.v1

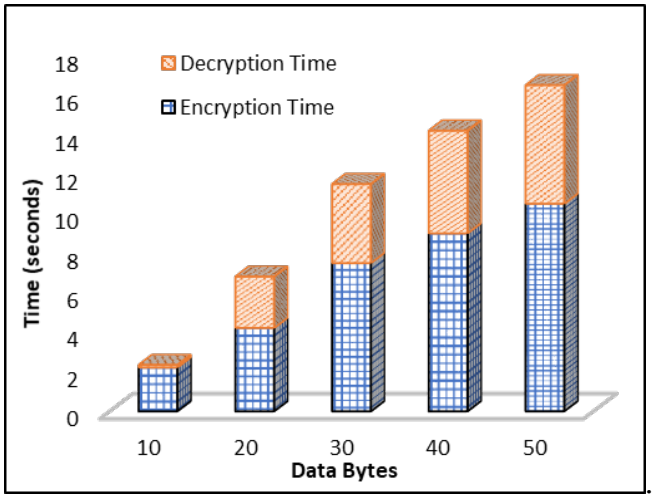

Figure 10. Time Complexity for Encryption and Decryption Algorithm.

4.5. Time Complexity Analysis for Encryption and Decryption Schemes

The encoding time of the different schemes are contrasted with the DEA's proposed algorithm. Compared to the other methods, Figure 11 shows that the data encryption process took less time for proposed algorithm. For encryption, DEA has lower time complexity. Multiple schema decryption time is checked because the suggested DEA algorithm has less time complexity compared to other data decryption schemes. The AES-CTR, ECC, and suggested DEA algorithms are timed, and it is discovered that AES-CTR takes about 40 seconds and has a lot of calculations, whereas DEA takes around 4 to 5 seconds and has a lot of computations.

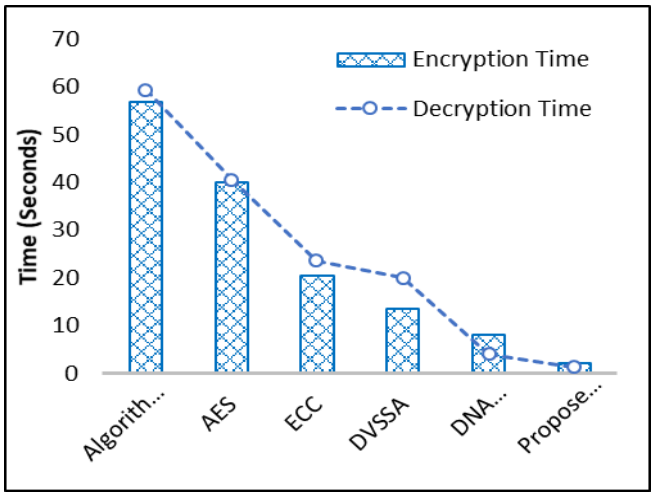

Figure 11. Time Complexity for Multiple Encryption and Decryption Algorithm.

In [35], the DNA based techniques demonstrate data security and its results are compared with the proposed DNA based technique as shown in Figure 13. In [36], DVSSA is used with DNA based method where data security and computational energy consumption is plotted in comparative analysis graph. In [37], various algorithms are used to secure data over the wireless network. Algorithm 4 is selected for the comparison because, it shows the less computational complexity. It is noted that overall, proposed DNA scheme took very less computational energy consumption as compared to all other related methods.

5. Discussion

With the high adoption rate of IoT in the medical field, sensors pose lots of concerns such as securing their data. Tackling such a concern is a challenge due to the limited resources of memory and energy in those devices. Different methodologies have been used to encrypt information, but these methodologies are not considered suitable for remote sensors due to scarcity of computing resources. In this work, we presented an approach that is based on the DEA cryptographic algorithm. To enhance this algorithm and make it more efficient, we used the ElGamal key generator. In CRNs, the routing protocol transmits data by utilizing the bandwidth of an idle spectrum. Results show that our approach is effective and efficient with respect to time complexity compared to its counterparts.

6. Conclusions

The proposed scheme is applied on the ECG-detected data to ensure secure data sharing. Data are encrypted and decrypted by the DNA-based process along with CRN protocol. It resolves the problem of interference and security attacks. CRN is used as a routing protocol to transfer the sensing data towards the biomedical server using bandwidth spectrum. CRNs sense idle spectrum in multiple antennas by using an improved energy detector. Secure DNA-based cryptographic mechanism protects against several security attacks. CRMBAN system gives approx. 90% better results in terms of complexity, time, and performance. The system is simulated using MATLAB 2013a. It also reduces power consumption. CRN for data routing will be efficient due to smooth data traffic. Experimental results show that no packet loss is observed by avoiding congestion of data traffic. Overall, the calculated results of the system are according to the requirements of the NSs capacity.

The proposed approach can be extended using different routing protocols and key approaches. To minimize the computational time it is imperative to have an algorithm with fewer steps. In future work, we will investigate DNA-based operations using fragmentation-based distributed cryptographic keys.

Author Contributions: All authors contributed equally and agreed to submit their work.

Funding: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R138), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Acknowledgments: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R138), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun and N. Jhanjhi, "Secure Healthcare Data Aggregation and Transmission in IoT—A Survey," IEEE Access, vol. 9, pp. 16849-16865, 2021.
2. M. A. Iliyasu, O. A. Abisoye, S. A. Bashir and J. A. Ojeniyi, "A Review of Dna Cryptograhic Approaches," IEEE 2nd International Conference on Cyberspac (CYBER NIGERIA), Abuja, Nigeria, 2021, pp. 66-72.
3. M. Khan and M. T. Jilani, "A security framework for wireless body areanetwork based smart healthcare system," in International Conference for Young Researchers in Informatics, Mathematics and Engineering, ICYRIME 201, Kaunas, Lithuania, 2017.
4. A. K. Shukla, P. K. Upadhyay, A. Srivastava and J. M. Moualeu, "Enabling Co-Existence of Cognitive Sensor Nodes with Energy Harvesting in Body Area Networks," IEEE Sensors Journal, vol. 21, no. 9, pp. 11213-11223, 2021.
5. D. Tarek, A. Benslimane, M. Darwish, A. M. Kotb, "Survey on spectrum sharing/allocation for cognitive radio networks Internet of Things, Egyptian Informatics Journal, vol. 21, no. 4, pp. 231-239, 2020.
6. D. Tarek, A. Benslimane, M. Darwish, A. M. Kotb, "A new strategy for packets scheduling in cognitive radio internet of things," Computer Networks, vol. 178, P. 107292, 2020.
7. X. Wang, X. Zhong, L. Li, S. Zhang, R. Lu, T. Yang, "TOT: Trust aware opportunistic transmission in cognitive radio Social Internet of Things, Computer Communications, vol. 162, pp. 1-11, 2020.
8. M. Shahfiq, H. Ashraf, A. U. llah and S. , "Systematic Literature Review on Energy Efficient Routing Schemes in WSN- A Survey," Springer Science+Business Media, p. 14, 2020.

9. K. A. Darabkh, O. M. Amro, R. T. Al-Zubi, H. B. Salameh, "Yet efficient routing protocols for half- and full-duplex cognitive radio Ad-Hoc Networks over IoT environment," Journal of Network and Computer Applications, vol. 173, P. 102836, 2021.
10. K. A. Darabkh, O. M. Amro, R. T. Al-Zubi, H. B. Salameh, R. Saifan, "JavaSim-IBFD-CRNs: Novel java simulator for in-band Full-Duplex cognitive radio networks over Internet of Things environment," Journal of Network and Computer Applications, vol. 172, P. 102833, 2020.
11. B. Bozorgchami and S. Sodagari, ""Spectrally efficient telemedicine and in-hospital patient data transfer,"," in 2017 IEEE International Symposium on Medical Measurements and Applications (MeMeA), Rochester, MN, USA, 2017 .
12. T. Manna and I. S. Misra, "Design, implementation and analysis of cognitive radio enabled intelligent WBAN gateway for cost-efficient remote health monitoring," Physical Communication, vol. 35, p. 27, 2019.
13. C. Tellambura and S. Kusaladharma, "An Overview Of Cognitive Radio Networks," Research Gate, vol. 8, no. 9, p. 18, 24 March 2018.
14. A. Aijaz and A. H. Aghvami, "Cognitive Machine-to-Machine Communications for Internet-of-Things: A Protocol Stack Perspective," IEEE Internet Things, p. 103–112., 2015.
15. A. Ali, W. Hamouda and M. Uysal, "Next Generation M2M Cellular Networks: Challenges and Practical Considerations," IEEE Commun. Mag., vol. 53, no. 9, pp. 18-24, June 2015.
16. A. F. Molisch, "Wireless Communications", USA: Wiley-IEEE Press; 2 edition, December 2010
17. A. A.-. Fuqaha, M. Guizani and . M. Mohammadi , ""Internet of things: a survey on enabling technologies,protocols, and applications,"," IEEE, vol. 17, no. 4, pp. 2347 - 2376, 15 June 2015.
18. Q. Wu, . G. Ding and Y. Xu, ""Cognitive internet of things: a new paradigm beyond connection,," " IEEE, vol. 1, no. 2, pp. 129 - 143, 12 March 2014.
19. M. S. Khan, J. Kim, E. H. Lee and S. M. Kim, "An Efficient Contention-Window Based Reporting for Internet of things Features In Cognitive Radio Networks," Wireless Communications and Mobile Computing, vol. 2019, p. 9, 18 Aug 2019.
20. S. Mohapatra, P. K. Sahoo and J. Sheu, "Spectrum Allocation With Guaranteed Rendezvous in Asynchronous Cognitive Radio Networks for Internet of Things," IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6104-6116, Aug. 2019,.
21. S. Djahel, A. Jones and Y. H.-. Aoul, "CRITIC: A Cognitive Radio Inspired Road Traffic Congestion Reduction Solution," in The 10th Wireless Days Conference (WD 2018), Dubai, UAE, Febrarury 2018, pp.151-157.
22. M. Indhumathi and S. Kavitha, "Distributed Intrusion Detection System for Cognitive Radio Networks Based on Weighted Fair Queuing Algorithm," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 3, no. 4, p. 11, 30-April-2020.
23. M. Amjad, M. H. Rehmani and S. Mao, "Wireless Multimedia Cognitive Radio Networks: A Comprehensive Survey," IEEE, p. 1056 - 1103, July 2018.
24. S. Bhattarai and J. Min, ""An overview of dynamic spectrum sharing: Ongoing initiatives, challenges,," IEEE Transactions, vol. 2, June 2016.
25. M. H. Rehmani and A. C. , "SURF: A distributed channel selection strategy for data dissemination in multi-hop cognitive radio networks," Computer Communications, vol. 36, no. 10-11, pp. 1172-1185, June 2013.
26. F. Tang, C. Tang, Y. Yang, L. T. Yang, T. Zhou and J. Li, "Delay-Minimized Routing in Mobile Cognitive Networks for Time-Critical Applications," IEEE Transactions on Industrial Informatics, vol. 13, no. 3, pp. 1398 - 1409, 2016.
27. A. S. Cacciapuoti, . M. Caleffi, . F. Marino and . L. Paura, "On the Route Priority for Cognitive Radio Networks," IEEE Transactions on Communications,, vol. 63, no. 9, pp. 3103–3117, 2015.
28. E. Etim and . J. Lota, "Power control in cognitive radios, Internet-of Things (IoT) for factories and industrial automation," in IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society, Florence, Italy, 22 December 2016.
29. T. Jabeen, H. Ashraf, A. Khatoon, S. S. Band and A. Mosavi, "A Lightweight Genetic Based Algorithm for Data Security in Wireless Body Area Network," IEEE Access, vol. 8, pp. 1-10, 2020.
30. J. Xu, X. Meng, W. Liang and H. Zhou, "A secure mutual authentication scheme of blockchain-based in WBANs," IEEE Access, vol. 17, no. 9, pp. 34 - 49, Sep 2020.
31. D. Rachmawati, M. A. Budiman and M. I. Wardhono, "Hybrid Cryptosystem for Image Security by Using Hill Cipher 4x4 and ElGamal Elliptic Curve Algorithm," in 2018 IEEE International Conference on Communication, Networks and Satellite (Comnetsat), Comnetsat, 2018.
32. Z. U. Rehman, S. Altaf and S. Iqbal, "An Efficient Lightweight Key Agreement and Authentication Scheme for WBAN," IEEE Access, vol. 8, no. 8, pp. 175385 - 175397, 24 September 2020.
33. L. XIAO, . D. HAN and X. MENG, "A Secure Framework for Data Sharing in Private Blockchain-Based WBANs," IEEE Access, vol. 8, no. 10, pp. 1-13, September 1, 2020.

34. Anwar M, Abdullah AH, Butt RA, Ashraf MW, Qureshi KN, Ullah F (2018) Securing data communication in wireless body area networks using digital signatures. Tech J Univ Eng Technol (UET) Taxila Pak 23(2):1–6
35. R. A. Ismail , H. Mohamed and M. E. Nasr, "Secure Image Encryption Scheme Based on DNA and New Multi Chaotic Map," Journal of Physics: Conference Series, vol. 1447, no. 14, pp. 1-12, 2020.
36. Y. Ren, Y. Leng, F. Zhu and J. Wang, "Data Storage Mechanism Based on Blockchain with Privacy Protection in Wireless Body Area Network," Sensors MDPI, vol. 2395, no. 19, p. 16, 2019.
37. Z. ZHAO, Y. BAN, D. CHEN and Z. MAO, "Joint Design of Iterative Training-Based Channel Estimation and Cluster Formation in Cloud-Radio Access Networks," IEEE Access, vol. 4, no. 20, p. 16, 2017.
38. Majid, M.; Habib, S.; Javed, A.R.; Rizwan, M.; Srivastava, G.; Gadekallu, T.R.; Lin, J.C.-W. Applications of Wireless Sensor Networks, and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review. Sensors 2022, 22, 2087. https://doi.org/10.3390/s22062087.