Computers, Materials & Continua
DOI:10.32604/cmc.2022.020016
Article

Tech Science Press

A Monte Carlo Based COVID-19 Detection Framework for Smart Healthcare

Tallat Jabeen[1,2], Ishrat Jabeen[1], Humaira Ashraf[2], Nz Jhanjhi[3,*], Mamoona Humayun[4], Mehedi Masud[5] and Sultan Aljahdali[5]

[1]Research Center for Modelling and Simulation (RCMS) NUST, Islamabad, 44000, Pakistan
[2]Department of Computer Science and Software Engineering, International Islamic University, Islamabad, 44000, Pakistan
[3]School of Computer Science and Engineering, SCE Taylor's University, Subang Jaya, 47500, Malaysia
[4]College of Computer Science and Information Technology, Jouf University, Al Jouf, Saudi Arabia
[5]Department of Computer Science, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
[*]Corresponding Author: Nz Jhanjhi. Email: noorzaman.jhanjhi@taylors.edu.my
Received: 06 May 2021; Accepted: 19 June 2021

Abstract: COVID-19 is a novel coronavirus disease that has been declared as a global pandemic in 2019. It affects the whole world through person-to-person communication. This virus spreads by the droplets of coughs and sneezing, which are quickly falling over the surface. Therefore, anyone can get easily affected by breathing in the vicinity of the COVID-19 patient. Currently, vaccine for the disease is under clinical investigation in different pharmaceutical companies. Until now, multiple medical companies have delivered health monitoring kits. However, a wireless body area network (WBAN) is a healthcare system that consists of nano sensors used to detect the real-time health condition of the patient. The proposed approach delineates is to fill a gap between recent technology trends and healthcare structure. If COVID-19 affected patient is monitored through WBAN sensors and network, a physician or a doctor can guide the patient at the right time with the correct possible decision. This scenario helps the community to maintain social distancing and avoids an unpleasant environment for hospitalized patients Herein, a Monte Carlo algorithm guided protocol is developed to probe a secured cipher output. Security cipher helps to avoid wireless network issues like packet loss, network attacks, network interference, and routing problems. Monte Carlo based covid-19 detection technique gives 90% better results in terms of time complexity, performance, and efficiency. Results indicate that Monte Carlo based covid-19 detection technique with edge computing idea is robust in terms of time complexity, performance, and efficiency and thus, is advocated as a significant application for lessening hospital expenses.

Keywords: COVID-19; coronavirus; cryptography; Monte Carlo algorithm; edge computing

1 Introduction

The COVID-19 has affected around 218 countries and territories worldwide, and the number of cases is still increasing daily. This coronavirus may affect an individual in various ways. For instance, some infected people may experience mild to moderate symptoms and might recover without hospitalization. The most common symptoms of the virus include temperature, cough, and breathing issues. COVID-19 is quickly transmitted through breath, cough, and sneeze droplets. The mortality and morbidity rate have reached unexpected levels in few months. To avoid this infection, various pharmaceutical companies are investing in the development of vaccines. However, development of a global vaccine is challenging and time demanding endeavor due to recent identification of new strain of COVID-19. However, self-isolation at home and immobilization may mitigate the risk of COVID-19. Nevertheless, airborne communication transmission can only be disinfected if appropriate handwashing procedures are followed, and precautionary measures are taken by each person to safeguard other individuals [1].

Therefore, social distancing is crucial to control the situation which could be maintained by opting real-time monitoring system. Multiple companies introduced COVID-19 diagnostics kits. The accuracy of the simple PCR kits remained gloomy. The IoT-based WBAN presents an opportunity to monitor the real-time status of the patient's health. WBAN consists of small sensors embedded over the human body that senses the health signs and transmits the record towards a biomedical server.

Consequently, a Monte Carlo algorithm guided protocol with security cipher has been proposed to monitor a patient's health and avoid frequent interaction with the hospital. First, the proposed algorithm calculates COVID-19 suspected patients' fitness based on the body temperature and breathing rate. There are random chances of COVID-19 positivity, negativity, and allergy. The data variable values are recorded and selected based on data sensing rate. After this, an efficient and very simple cipher algorithm is applied over the randomly chosen status of human health. The security algorithm used a very simple procedure for the key generation that is used in the encryption and decryption process.

The proposed COVID-19 detection technique gave 90% efficiency terms of time complexity, various attack resistance, and network congestions problems.

The contribution of this article is summarized as follows.

- This work provides COVID-19 detection along with the WBAN transmission framework.
- Secure approach is used to transmits data to the data analyst and a doctor.
- A random selection algorithm is used to exactly identify the real time health status at any time
- It provides a real-time monitoring system to limits the spread of viral disease.
- Edge computing brings biomedical server closer to transmitter and decrease response time.

The rest of the article is organized as Section 2 provides a literature review, Section 3 contains methodology, Section 4 presents results and analysis, and Section 5 shows the discussion and future work.

2 Literature Survey

This section provides COVID-19 based literature and WBAN based cryptographic techniques along with cognitive radio networks (CRN) protocol.

In Wuhan, China, several unidentified cases of pneumonia have appeared in 2019. A new coronavirus, dubbed COVID-19, was discovered in a series of deep studies on respiratory tract samples. To date, in 210 different countries and territories around the world, more than 19,193,980 patients have been registered. Therefore, to clarify the essence of the virus, numerous medical and non-medical experiments have been performed [2].

Coronaviruses are positive non-segmented RNA viruses that belong to the family of coronaviridae which are widely distributed to humans and mammals [3]. Second, multiple studies have been carried out to find a link between the progression of COVID-19 and other variables such as age, heart disease, etc. In [4,5], the authors stated that age is one of the key risk factors for complications of diseases. To analyze this data, Saeed et al. [6] used a data mining technique of extracting correlation between smoking and COVID-19 infection. Multiple studies focused on machine learning and deep learning for the detection of COVID-19 patients [7]. Ozturk el al. [7] proposed a Dark Net Convolutional Neural Network (CNN) based deep learning model on the 125 chest X-rays and find good results percentage in detecting COVID-19 disease. Another article intended to employ 150 CT images used for the detection of COVID-19 disease [8].

Smart sensors act as a bridge between patients and healthcare devices that collect human health data and forward it towards the doctor or a physician [9]. The main goal of sensor networks' design is to capture and interpret data in real-time in hostile environments or dangerous areas where access to human resources is not feasible. Because of this Senor network property, they are used in various control and monitoring applications such as healthcare systems, battlefields, terrains, simulations, nuclear sites, space, etc. [10]. The tracking of vital safety data in e-health research has become a major challenge as WBAN deals with multiple threats day by day. Therefore, today's need is to design safe and resource-optimal algorithms with a robust key generation and management framework [11].

The authors improved the IJS algorithm for calculating coefficients (encoding) and restoring minor data errors in [12]. The relatively insecure on-body channels (between the control unit and non-line-of-sight nodes) are exploited in [13] to extract secret keys from channel features for safe communication between two on-body devices. A realistic, reliable, effective, characteristic-based, cooperative key generation method for communication links were suggested in [14] to increase the key generation rate for restricted nodes that can borrow resources from assistant nodes for their key generations.

The fuzzy vault scheme that generates the polynomial to encode the hidden information was proposed by Liu et al. [15]. For safe communication, Babu et al. [16] have provided the WBAN hybrid security procedure. The concept of water rendering ECG-based signal tempering was proposed by Kaur et al. [17]. Jabeen et al. [18] proposed a genetic-based encryption algorithm for data security with an efficient and lightweight MQTT protocol in WBAN. Reference [19] provides better survey for multiple safety schemes to present comparison analysis and security parameters.

3 Problem Statement

The problems obtained from the literature survey along with the solution given through COVID detection architecture and security cipher are stated in this section.

There should be a procedure for (COVID suspected) patients that helps the community to maintain social distancing and avoids an unpleasant environment for hospitalized patients.

To augment the security of data transmission in WBAN's, multiple ciphertext algorithms are being used previously. However, [11] various were mainly influenced by the DOS types of attacks [12]. Therefore, a secure encryption technique with less memory consumption and efficient data security ratio may advocate a novel strategy to evade attacks and maintain smooth data transmission.

Solution:

Here, we proposed a logical system for COVID detection procedure that helps to detect patient's real time health status through sensors and transmits data with secure cipher. A security algorithm along with an efficient network protocol is proposed to avoid various malicious attacks to maintain even data transmission. Proposed wireless radio network protocol is also helps to evade wireless network issues e.g., data congestion and traffic load.

4 The Architecture of COVID-19 Detection Through WBAN

Fig. 1 presents the proposed architecture of WBAN that contains three layers. The first layer used sensors to detect record of patient's health based on body temperature and respiratory or breathing level. Based on these variables, COVID-19 positive, negative, or simple allergic problem can be predicted with reasonable accuracy. To avoid wireless network issues, the sensor's data could be secured with the help of the cipher algorithm. Briefly, the encrypted data is collected by the mobile node and transferred towards the second layer of the access point. Here, encrypted data can be forwarded by an edge computing device directly to the server and if there is no sufficient storage, then data is moved to the internet cloud. Edge computing brings the server closer and saves bandwidth for data delivery. This data moved to a biomedical server through internet cloud and edge computing devices, where the data analyst may decrypt the data for the understanding of a physician or doctor.

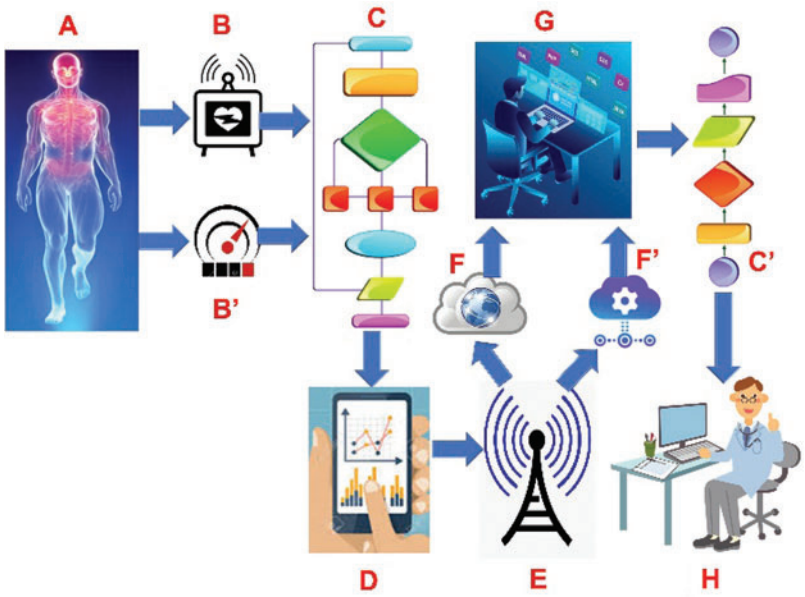

Figure 1: The architecture of COVID-19 detection through WBAN. (A) reflect a patient, (B) and (B') represent breathing rate and temperature nano sensors, respectively. C and C' shows that simple sensor's detected data passes through proposed encryption and decryption algorithm, respectively. D is the mobile node that receive encrypted data from both sensors. E. represents access point which transfers the encrypted data to F (internet cloud) and F' (edge computing). G is the data analyst who decrypt the received data by C' and transfer the data to doctor (H)

Encryption and Decryption Procedure

The proposed study's main objective is to provide a complete structure that restricts the spread of COVID-19. It focuses on early detection and isolation, as these are the most significant factors that may help to minimize the number of cases of COVID-19. It is possible because of tracking patient's vital signs through wearable sensors, and this will easily prevent unpleasant situations for hospitalized patients and doctors. Consequently, a random selection Monte Carlo based algorithm is proposed to detect the COVID signs and secure them with a simple encryption algorithm to forward over the sensor network. The recommended structure is divided into three categories sensors detection, cognitive routing network protocol, and hospital or doctor side layer.

Nano sensors detected humans' real-time health status based on the suggested parameters such as body temperature and respiratory rate. Tab. 1 shows the health signs in comparison of COVID-19 affected patient and normal or usual healthy person. It is observed that the body temperature of COVID patient is 38 to 40°C while in comparison the healthy patients have 36.5 to 37.2°C. Breathing or respiratory rate of COVID active patients have 30 or more breaths per minute and the normal healthy patient contains a respiratory rate of 12 to 16 breaths per minute.

Table 1: Health signs of Covid *vs*. healthy patient's

Symptoms/signs	Normal/usual range	COVID-19 active range
Temperature C°	Up to 36.5 to 37°C	38 to 40°C
Respiratory/breathing rate	12 to 16 breaths per minute.	Respiratory rate of 30 or more breaths per minute.

COVID-19 suspected patients' health based on the temperature and respiratory parameters is calculated and resultant options are achieved. Fig. 2 shows a Monte Carlo based algorithm that has three possibilities of COVID positive, COVID negative, and Allergic conditions of human health. Therefore, the proposed scheme randomly selects anyone's real-time health status and process encryption algorithm procedure to avoid network issues. Randomly selection of health status acts as an input for the encryption process. Firstly, convert the input alphabets into corresponding numeric values e.g., A = 0, B = 1, and C = 2,..., Z = 25. Now convert these numeric values into 8-bits binary and perform XOR logical operation with the key generated 8-bit binaries. Then heat map method is implemented over the resultant's binaries. There are two colors 'red' and 'green' are selected for every bit of binary, all the 1's are converted into red color and all 0's in the string are converted into green color. Red and green colored string is ciphertext which is ready for transmission over the network.

Tab. 2 presents substitution bits (SB Box) values that are used to shuffle bits of randomly chosen integers after binary conversion. These values are used as a key value in the encoding and decoding process of the algorithm.

In the Decryption process, all the encryption steps are reversed at the physician's server-side. Ciphertext heat map colors are converted into their corresponding binary values and perform XOR logical operation with the key values. Resultant binary values are converted into numeric values which are substituted with the corresponding alphabets. This alphabet string was an input of the algorithm.

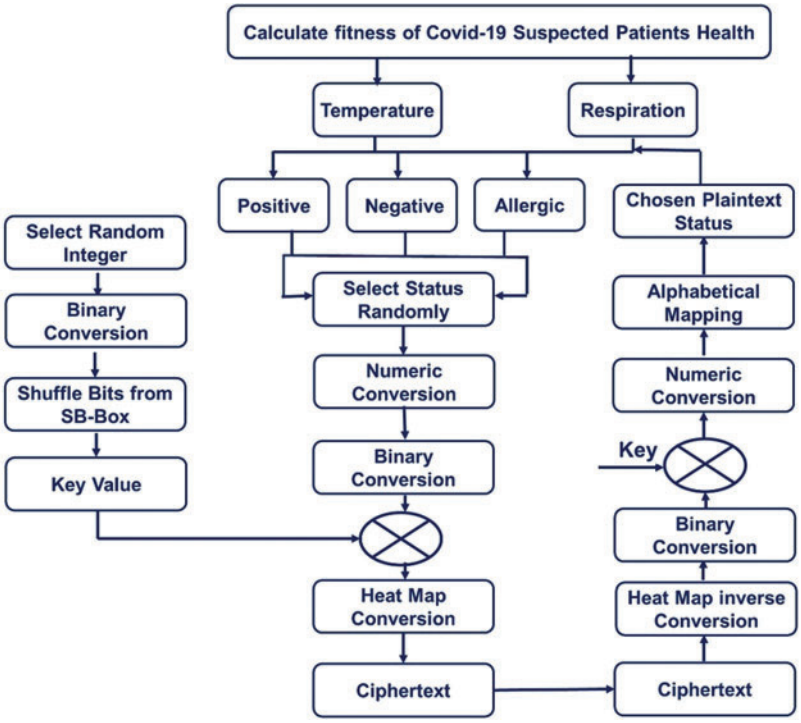

Figure 2: Monte Carlo based security procedure

Table 2: S-Box for key generation process

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**

Tab. 3 presents the encryption and decryption algorithm in the step-by-step procedure, starting from calculating fitness and performing various operations to generate the ciphertext. The applied simple operations are effective to secure patient's data over the wireless network.

Fig. 3 shows the framework of the WBAN and cognitive radio network (CRN) protocol. CRN used multiple bandwidth spectrum paths for routing the WBAN's data over the network. Body node coordinator (BNC) used idle bandwidth spectrum for the data transmission towards edge computing.

If there is not sufficient space for data storage is left, then data forwarded to the internet cloud which relates with the biomedical server else simply data will be transmitted to the server from an edge computing device. Doctor or physician easily get access to the encrypted data which is decrypted by the medical server in a very less amount of time. After fetching original or plain data, the physician can advise further treatments to keep maintaining social distancing. This strategy will avoid network congestion issues, maintains security, and original data for the doctor analysis.

Table 3: Proposed algorithm with key generation procedure

Key Generation:
Setup of nodes, the base station Select any integer value. Convert into binary Apply shuffle bits from SB BOX key value
Encryption:
Calculate fitness of patient Respiratory and temperature range Resultant health status Select random input Convert $\in$ into 8 bits numeric values $\boldsymbol{temp1}^{\in\prime}$ = Binary Conversion $\text{temp2}^{\in\prime} = \overline{Key \bigoplus^{\in\prime}}$ (take XOR with key generated above with plaintext) $\boldsymbol{temp3}^{\in\prime}$ = Heat map $\text{Temp4}^{\in\prime}$ = Ciphertext
Decryption:
Conversion of ciphertext into plaintext: $\text{Convert}^{\in\prime}$ into binary values (Green as '0' and Red as '1') $\text{temp1}^{\in\prime} = \overline{Key \bigoplus^{\in\prime}}$ (take XOR with key generated) $\text{temp2}^{\in\prime}$ = Numeric Conversion $\text{temp3}^{\in\prime}$ = Alphabetical mapping $\boldsymbol{temp4}_{\in\prime} = Plaintext$

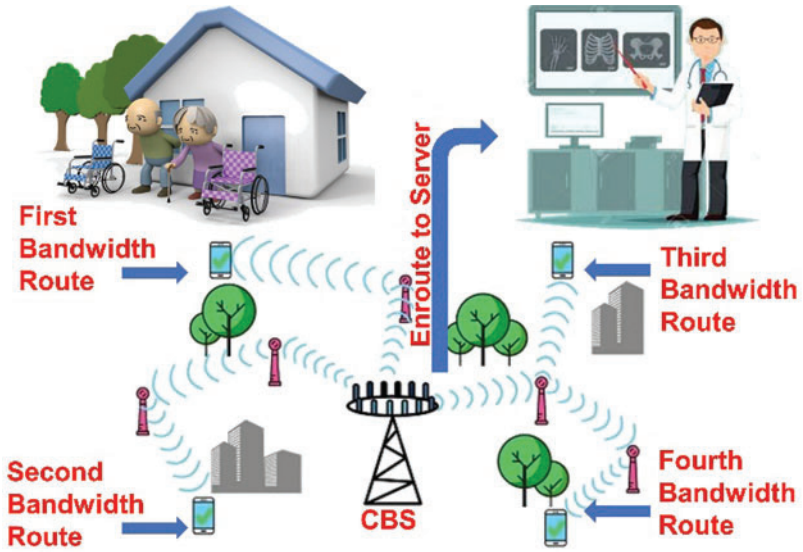

Figure 3: COVID detection with WBAN's sensors over CRN layout

Fig. 4 demonstrated the data routing procedure for a wireless cognitive radio network protocol. Sensor sensed data and calculated ciphertext by implementing various operations and transmits through the idle bandwidth routing spectrum. Additionally, this path further routes data towards edge computing, and then to the biomedical server.

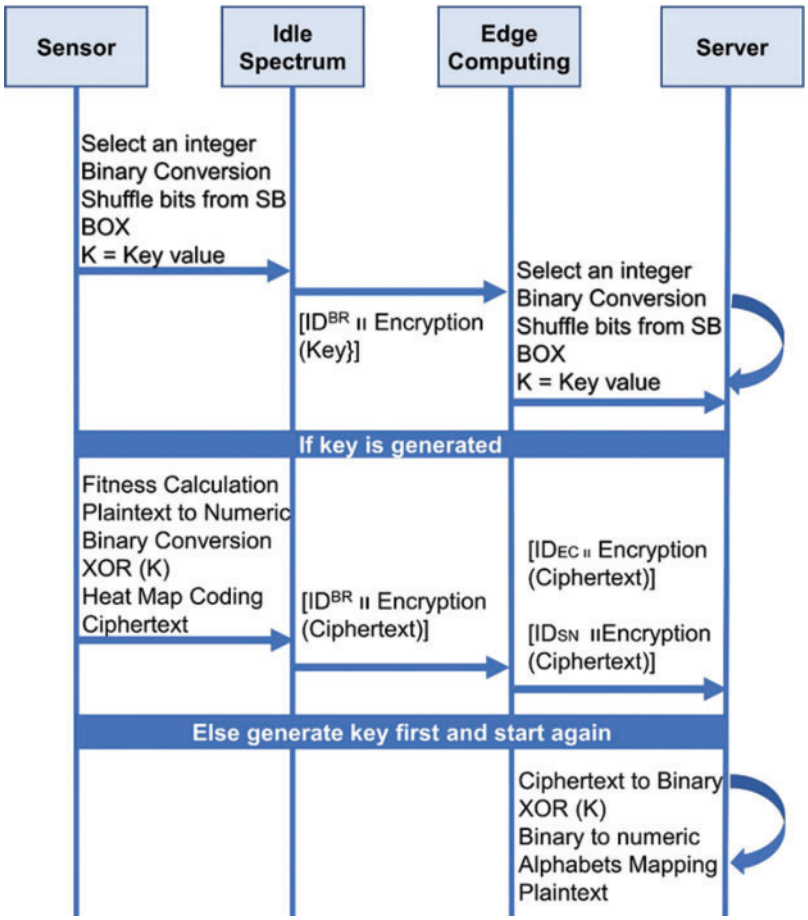

Figure 4: Routing COVID detected data over CRN protocol from sensor originators towards receiver server

Mathematical Modeling

$$F = T + R \tag{1}$$

F is calculating the fitness of COVID suspected patients based on the temperature and respiratory or breathing parameters. If temperature and breathing pace is up to the level of the proposed rate, then sensors detect the fitness of the patient.

$$F' = P\,|N|\,A \tag{2}$$

F' are resultant choices for the detected parameters rate, either it is COVID positive, negative, or maybe simply allergic condition is detected. F' simply select any health status randomly and proceeds with the encryption steps.

$$X = F' \rightarrow Zn \tag{3}$$

$$X1 = Zn \rightarrow Bi \tag{4}$$

X is the provisional data that is updated according to the applied operations. Here, X is converting randomly chosen to input into their corresponding numeric form which is Zn. X1 stores the binary input data converted from Zn.

$$X2 = Bi \oplus K \tag{5}$$

Binary input data perform XOR logical operation with the key-value generated from the simple procedure and the resultant data is updated in X2.

$$X3 = X2 \rightarrow Hm \tag{6}$$

$$X3 = Cipher \tag{7}$$

X3 updates data by implementing heat map conversion on the temporarily generated data of X2. It converts binaries of '0' into green color and '1' into red color. This red and green colored generated string is the ciphertext that is kept into the X3.

5 Results and Discussion

The proposed COVID-19 detection and transmission methodology procedure is analyzed in the MATLAB environment. A Monte Carlo based algorithm is used to randomly select the health status of the suspected patient by the sensors. There are simple encryption steps are also computed to avoid network interference issues. Experimental results are calculated over the MATLAB based on the encryption and decryption time consumption.

5.1 Computational Time

The computational time is the total time taken by a specific algorithm to compute its results. For an encryption approach, the computational time is a critical output parameter that illustrates how many times a certain operation takes to execute within one protocol transaction.

5.2 Computational Time of Key Generation

The proposed key generation algorithm has a simple and quickly performed procedure that generates key value for the encryption and decryption process.

Fig. 5 shows that computational time for the key generation procedure is low and has a quick response. It is noted that as the data byte for the input value is increased the time in milliseconds increased too, but the time taken to compute the key for encryption and decryption process is very less.

5.3 Computational Time of Encryption

The computational time taken by the Monte Carlo based algorithm is calculated. It has a very simple and efficient procedure to encrypt patient's data to avoid network interference issues.

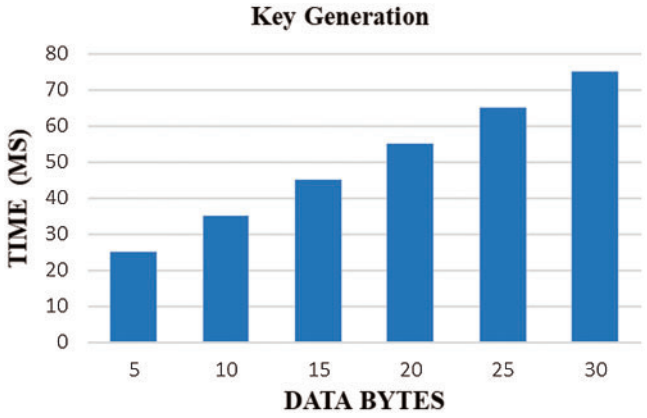

Figure 5: The time complexity for the key generation algorithm

Fig. 6 presents the encryption time taken by the proposed algorithm to compute efficiency results. When the input data bytes increase the time taken by the algorithm also increased, generally the time complexity for the encryption of a patient's record is minimal in the proposed scenario.

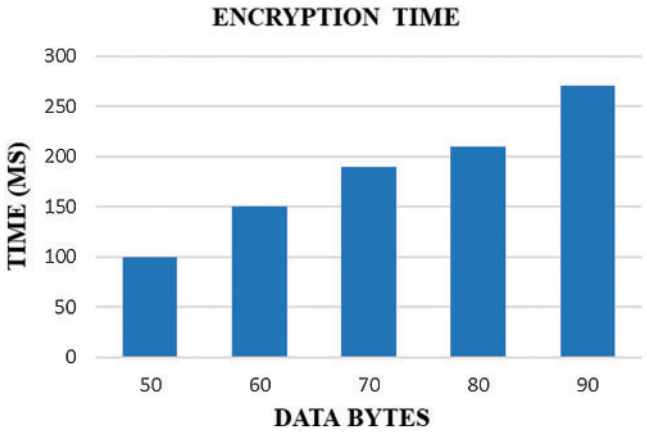

Figure 6: Time complexity for the encryption algorithm

5.4 Computational Time of Decryption

Computational time taken by the proposed monte Carlo based algorithm to decrypt the ciphertext at the server side is calculated. It follows simple technique to decode ciphertext into the original data.

Fig. 7 demonstrated that decoding time of ciphertext is increased in milliseconds by increasing the output data bytes. It is reflected that overall time taken is very low and the proposed algorithm is efficient.

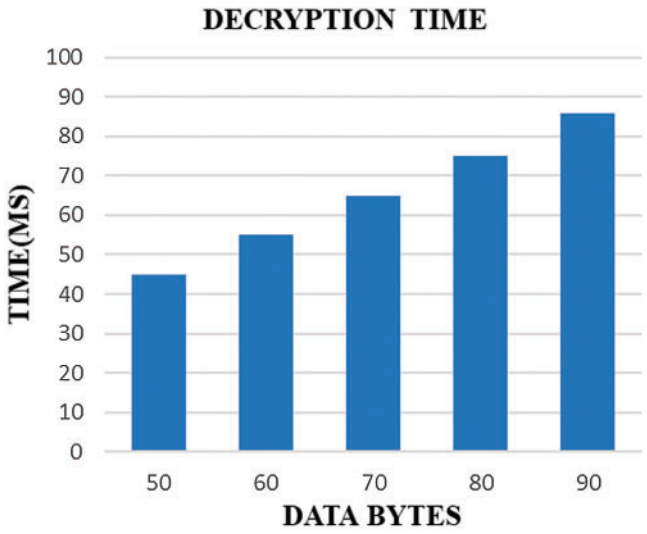

Figure 7: Time complexity for decryption algorithm

5.5 Comparison Analysis for Key Generation Algorithm

A comparison analysis of the proposed key generation algorithm is performed with the Kumar et al. [20]. Fig. 8 shows that the computational time taken by the Diffie-Hellman technique to generate a key is higher than the time taken by the proposed scheme.

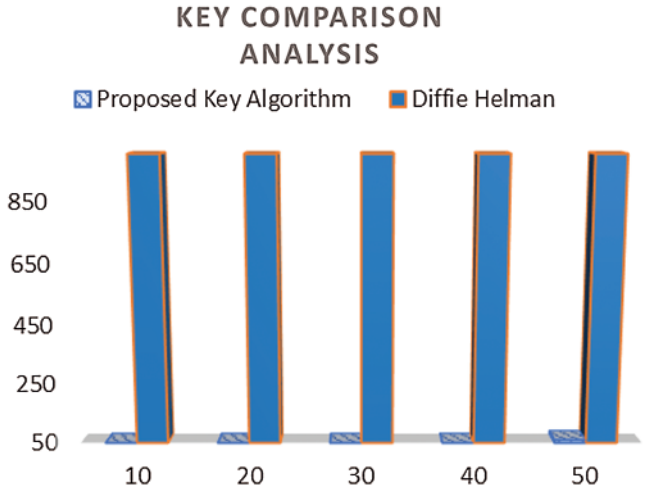

Figure 8: Time complexity for key comparison analysis

5.6 Comparison Analysis for Encryption and Decryption Algorithm

Comparison analysis of various techniques with the proposed scheme is performed to check the efficiency of algorithm. Fig. 9 reveals that proposed monte Carlo based algorithm took less computational time as compared to other techniques. Encryption and decryption computational time complexity is clearly lesser than in compared algorithms ECC [20] and AES [21].

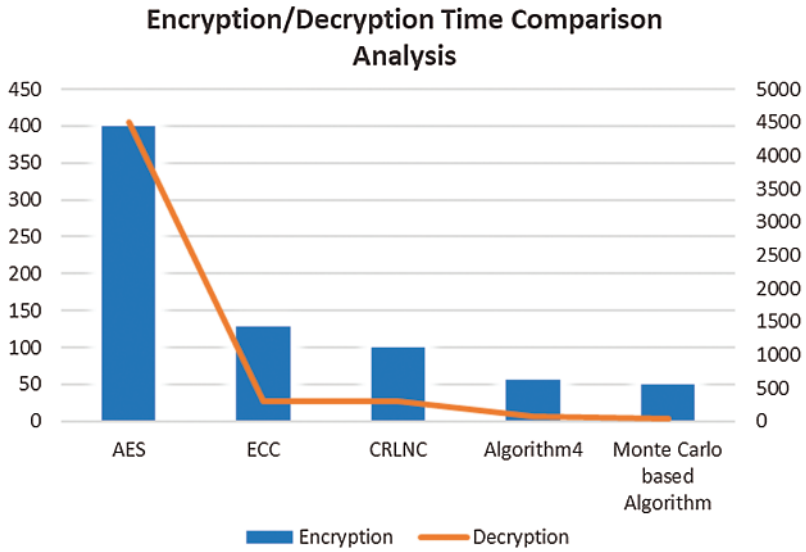

Figure 9: Time complexity for encryption and decryption comparison analysis

5.7 Comparison Analysis for Routing Protocol

Cognitive radio (CR) is a kind of wireless communication in which a transceiver can detect intelligently which channels of communication are in use and which are not. It moves into empty channels immediately while avoiding populated ones. The certified users do not cause any interference. Cognitive radio networks as a wireless protocol avoids traffic congestion over the network to make sure the smooth data transmission. Here, by using this protocol disadvantage of data transmission delay is also avoided.

Multiple wireless communication protocols are used such as WIFI, Zigbee, Bluetooth or NFC. The major problem with Zigbee protocol is the insecure key exchange concern [22]. Various other protocols like Wi-Fi and Bluetooth are used for the very short range and not suitable for the proposed scenario.

6 Security Analysis

6.1 Plaintext Attack

In Cryptography, known plaintext attack is very basic and common kind of interrupt in data transmission. The intruder or interrupter strive to analyze the relationship between known chunk of plaintext and ciphertext. Through this process, attackers try to access the whole proposed algorithm and manipulate the detected data.

$P(E(T,R)) = (Z(E,P),(M,R)$ where P is the plaintext and E shows encrypted data, T is the transmitter that transmits data towards receiver R. Z is the attacker that tries to retrieve plaintext from the encrypted or cipher data and forward manipulated data M to the receiver.

Simply, plaintext or original data is not sending over the recommended network. The proposed technique avoids this common attack by providing encryption and decryption process with the key generation scheme.

6.2 Eavesdropping Attack

Eavesdropper is the man-in-middle that injects fake data packets into the smooth data transmission. Intruder or attacker listen the conversation between sender to receiver secretly.

(E (T, R)) = $Z(E_i(R))$ Where E is the encrypted data that is used to communicate between sender T and receiver R. Z is the attacker that injects fake data continuously and forward it towards receiver.

The proposed algorithm avoided this man-in-middle because of an efficient secret key sharing process.

6.3 Collision Attack

In this scenario, attacker may intentionally forward the dummy packets to collide the important data that cause collision. This attacker discards the original data by targeting fake data.

(E (T, R)) = (Z (F, E)) Where E is the encrypted data that is used to transfer between transmitter T and receiver R. Z is the attacker or intruder that simply discard encrypted data by hitting fake data F.

The proposed technique avoided this attack by introducing CRN protocol. CRN used idle bandwidth spectrum and only licensed personal can access the path.

6.4 Jamming Attack

Jamming attack interrupts with the node frequencies and it is the DOS (Denial of service) type attack. Attackers distract smooth data transmission between sender and receiver, flow of data is diverted to another path by the attacker instead of receiver path.

(NS, NR) = (NS), (Z(NR)) where NS is sender node and NR are a receiver node. Z is jamming attacker that interrupts the data transmission.

Because of CRN, the proposed approach avoids this attack. For data transmission, a cognitive network uses a priority-based and empty bandwidth spectrum. This concept does not obstruct the data transmission channel. Furthermore, due to the adaption of the idle spectrum, data collision has been avoided.

6.5 Tempering Attack

Tempering is an attack in which an attacker is allowed physical access to a node, or an interloper can access sensitive information on the node, such as cryptographic secret keys or other classified material. At that moment, the system is confined by the invader, who can modify, or communication is replaced. Outsider Z is broken down by communication between nodes A and B, allowing physical access to data transmission.

Proposed technique avoided this attack because of encryption and decryption along with key generation steps. Attacker would not be able to get plaintext without knowing key and encryption procedure (NA, NB) = (Z(NA)), (Z (NB)).

6.6 Selective Repeat Attack

A node acts as a router, and hostile nodes can refuse to forward certain messages and simply dump them in a selective forwarding attack.

It also has an impact on the seamless transfer of data over the network. It shows how the selective node ZS disrupts transmission between sender NS and receiver node NR, and how

the data packets are affected by the selective faked packet by the attacker ZA as (NS, NR) = ((NS)(ZS)) ((ZA) + (NR)

This assault was intercepted by the proposed technique, which included an encryption and decryption method that prevented this type of attack from affecting the original data. As a result, the receiver rejects selectively sent packets.

7 Conclusion

The proposed Monte Carlo based algorithm is applied over the COVID-19 patient's data. Patient's real time health status is randomly chosen by the algorithm and encrypted with the very efficient procedure. Sensors transmits the encrypted data towards doctor over a wireless channel to maintain safe distance from the people. Cognitive wireless network is used as a protocol to communicate with the server. Edge computing device is introduced between bandwidth data path and server which reduce time and bring server closer. Monte Carlo based covid-19 detection technique gives 90% better results in terms of time complexity, performance, and efficiency. This system is implemented over MATLAB 2013a and evaluation measures are taken. Overall, the computational results of the proposed system are according to the sensors capacity.

8 Discussion and Future Work

Coronavirus (COVID-19) is a new pandemic disease that effects human by sneezing and cough droplets over the surface. This disease could be avoided by maintaining social distancing. Hence the WBAN is used for the patients to prevent unpleasant environment in hospitals. WBAN is a wireless network that used tiny sensors to sense the real time health status of the patients. Nano-sensors are the wearable devices which are implanted over the human body that detects the human vital signs and transmits on the network. Security is the leading issue in wireless system to protect against various attacks and network interferences. Therefore, wireless network data should be in an unpredictable or in ciphertext form. Several literature articles proposed security algorithms to encrypt and decrypt the collected data, many of them contains some stumbling blocks of heavy computations. Consequently, proposed Monte Carlo based algorithm along with very simple and an efficient encryption procedure used for the detection of COVID patients. Routing protocol used for data transmission is CRN which choose empty available routing path. Results shows that proposed algorithm is an efficient scheme in terms of computational complexity and security concerns.

The proposed approach can be extended by introducing a decent authentication procedure for the patients to avoid unauthorized personal in the system. Proposed methodology can also be prolonged by implementing another efficient encryption and decryption algorithm along with key generation combination. A better solution could be provided to avoid various other wireless networks problem.

Acknowledgement: The authors would like to thank for the support from Taif University Researchers Supporting Project number (TURSP-2020/73), Taif University, Taif, Saudi Arabia.

Funding Statement: Taif University Researchers Supporting Project number (TURSP-2020/73).

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

References

[1] K. Abid, Y. A. Bari, M. Younas and S. T. Javaid, "Progress of COVID-19 epidemic in Pakistan," *Asia Pacific Journal of Publich Health*, vol. 32, no. 4, pp. 3–18, 2020.

[2] S. E. Sappagh, N. E. Rashidy and S. M. R. Islam, "End-to-end deep learning framework for coronavirus (COVID-19) detection and monitoring," *MDPI Electronics*, vol. 9, no. 9, pp. 1–25, 2020.

[3] A. R. Falsey and E. E. Walsh, "Novel coronavirus and severe acute respiratory syndrome," *PMID*, vol. 361, pp. 1312–1313, 2019.

[4] Y. Dong and Xi Mo, "Epidemiology of COVID-19 among children in China," *Pediatrics*, vol. 145, no. 6, pp. 1–12, 2020.

[5] H. W. Jeong, J. Y. Heo and H. W. Kim, *Persistent Environmental Contamination and Prolonged Viral Shedding in Mers Patients during Mers-Cov Outbreak in South Korea*. vol. 2. Oxford University Press, US national library of medicine national institutes of health, pp. 1978a, 2015.

[6] S. Saeed, N. Z. Jhanjhi, M. Naqvi, M. Humayun and V. Ponnusamy, "Quantitative analysis of COVID-19 patients: A preliminary statistical result of deep learning artificial intelligence framework," in *ICT Solutions for Improving Smart Communities in Asia*, 1st ed., vol. 1. Hershey, Pennsylvania, USA: IGI Global, pp. 218–242, 2021.

[7] T. Ozturk, M. Talo, E. A. Yildirim and U. B. Baloglu, "Automated detection of COVID-19 cases using deep neural networks with X-ray images," *Computer in Biology and Medicine*, vol. 121, no. 1, pp. 11, 2020.

[8] M. Barstugan, U. Ozkaya and S. Ozturk, "Coronavirus (COVID-19) classification using CT images by machine learning methods," *ACM*, vol. 542, no. 7639, pp. 10, 2020.

[9] H. Versteeg, S. S. Padersen, M. H. Mastenbroek and W. K. Redekop, "Patient perspective on remote monitoring of cardiovascular implantable electronic devices: Rationale and design of the REMOTE-CIED study," *Netherlands Heart Journal*, vol. 10, no. 8, pp. 423–428, 2014.

[10] S. Farooq, D. Prashar and D. KiranJyoti, "Hybrid encryption algorithm in wireless body area networks (WBAN)," *Intelligent Communication Control and Devices*, vol. 624, no. 1, pp. 401–410, 2019.

[11] S. J. Hussain, M. Irfan, N. Z. Jhanjhi, K. Hussain and M. Humayun, "Performance enhancement in wireless body area networks with secure communication," *Wireless Personal Communications*, vol. 116, no. 1, pp. 1–22, 2021.

[12] Z. Li and H. Wang, "A key agreement method for wireless body area networks," in *Proc. INFOCOM WKSHPS*, San Francisco, CA, USA, pp. 690–695, 2016.

[13] L. Shi, J. Yuan, S. Yu and M. Li, "MASK-BAN: Movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks," *IEEE Internet of Things Journal*, vol. 2, no. 1, pp. 52–62, 2015.

[14] Z. Li, H. Wang, M. Daneshmand and H. Fang, "Secure and efficient key generation and agreement methods for wireless body area networks," in *Proc. ICC*, Paris, France, pp. 1–6, 2017.

[15] J. Liu and K. S. Kwak, "Hybrid security mechanisms for wireless body area networks," in *Proc ICUFN*, Jeju, South Korea, pp. 98–103, 2010.

[16] A. M. Babu and K. J. Singh, "Performance evaluation of chaotic encryption technique," *American Journal of Applied Sciences*, vol. 10, no. 1, pp. 35–41, 2013.

[17] S. Kaur, R. Singhal, O. Farooq and B. S. Ahuja, "Digital watermarking of ECG data for secure wireless communication," in *Proc. ICRTIT*, Kochi, Kerala, India, pp. 140–144, 2010.

[18] T. Jabeen, H. Ashraf, A. Khatoon, S. S. Band and A. Mosavi, "A lightweight genetic based algorithm for data security in wireless body area networks," *IEEE Access*, vol. 8, no. 1, pp. 1–10, 2020.

[19] T. Jabeen, H. Ashraf and A. U. llah, "A survey on healthcare data security in wireless body area networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 8, pp. 14, 2021.

[20] V. Kumar, R. Kumar, M. A. Barbhuiya and M. Saikia, "Multiple encryptions using ECC and its time complexity analysis," *International Journal of Computer Engineering in Research Trends*, vol. 3, no. 11, pp. 568, 2016.

[21] F. S. Chowdhury, A. Istiaque, A. Mahmud and M. Miskat, "An implementation of a lightweight end-to-end secured communication system for patient monitoring system," in *Proc. EDCT*, Kolkata, India, Guru Nanak Institute Technology, pp. 15, 2018.

[22] D. S. Pereira, M. R. Morais, L. B. Nascimento, P. J. Alsina, V. G. Santos *et al.,* "Zigbee protocol-based communication network for multi-unmanned aerial vehicle networks," *IEEE Access*, vol. 8, no. 1, pp. 57762–57771, 2020.