Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.024605
Article

Tech Science Press

Neural Cryptography with Fog Computing Network for Health Monitoring Using IoMT

G. Ravikumar[1], K. Venkatachalam[2], Mohammed A. AlZain[3], Mehedi Masud[4] and Mohamed Abouhawwash[5,6,*]

[1]Department of Computer Science and Engineering, Coimbatore Institute of Engineering and Technology, Coimbatore, 641109, India
[2]Department of Applied Cybernetics, Faculty of Science, University of Hradec Králové, 50003, Hradec Králové, Czech Republic
[3]Department of Information Technology, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif, 21944, Saudi Arabia
[4]Department of Computer Science, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif, 21944, Saudi Arabia
[5]Department of Mathematics, Faculty of Science, Mansoura University, Mansoura, 35516, Egypt
[6]Department of Computational Mathematics, Science, and Engineering (CMSE), Michigan State University, East Lansing, MI, 48824, USA
*Corresponding Author: Mohamed Abouhawwash. Email: abouhaww@msu.edu
Received: 24 October 2021; Accepted: 24 January 2022

Abstract: Sleep apnea syndrome (SAS) is a breathing disorder while a person is asleep. The traditional method for examining SAS is Polysomnography (PSG). The standard procedure of PSG requires complete overnight observation in a laboratory. PSG typically provides accurate results, but it is expensive and time consuming. However, for people with Sleep apnea (SA), available beds and laboratories are limited. Resultantly, it may produce inaccurate diagnosis. Thus, this paper proposes the Internet of Medical Things (IoMT) framework with a machine learning concept of fully connected neural network (FCNN) with k-nearest neighbor (k-NN) classifier. This paper describes smart monitoring of a patient's sleeping habit and diagnosis of SA using FCNN-KNN+ average square error (ASE). For diagnosing SA, the Oxygen saturation (SpO2) sensor device is popularly used for monitoring the heart rate and blood oxygen level. This diagnosis information is securely stored in the IoMT fog computing network. Doctors can carefully monitor the SA patient remotely on the basis of sensor values, which are efficiently stored in the fog computing network. The proposed technique takes less than 0.2 s with an accuracy of 95%, which is higher than existing models.

Keywords: Sleep apnea; polysomnography; IOMT; fog node; security; neural network; KNN; signature encryption; sensor

1 Introduction

The Internet of Medical Things (IoMT) is the amalgamation of medical applications using sensor devices to connect with health-related information. In this scenario, user health data are sensed by the

IoMT and transferred to the chief physician through a modern communication system. Even without the physical presence of the patient, the doctor can naturally view his or her health condition to prescribe medication. Thus, transferring and storing the sensitive data must be secured.

Sleep is one of the fundamental daily needs and is significant for brain function. Any sleep disorder can naturally affect general health and cause serious health problems, such as brain stroke, high blood pressure, complicate daily activities, and risk safety. Experts use Polysomnography (PSG) to study sleep disorders. PSG is a collection of signals recorded from various sensors counting the Electroencephalogram (EEG), Electro oculography (EOG), Electromyogram (EMG), Electrocardiogram (ECG), airflow, thoracic and abdominal movements, and oximetry. Rechtschaffen and Kales standardized the sleep stage classification rules depending on EEG modifications and split Non-Rapid Eye Movement (NREM) in sleep is a natural relief of humans and prevents several diseases. Sleep apnea is a sleep disorder in which breathing problem occurs during sleep states. SA affects our health by decreasing the oxygen blood level, eventually leading to other diseases [1]. SA impacts our health, mentally and physically, causing diseases, such as stroke, cardio problems, and diabetes. Scientifically, based upon the international sleep expert's key observation, roughly one billion people worldwide have obstructive sleep apnea (OSA) [2].

IoMT collects significant health-related data and helps early diagnosis of diseases using machine learning techniques. Persons health data is considered extremely sensitive and confidential to users. Thus, IoMT must ensure user privacy [3] through a federated learning technique. This learning method trains the device to stop sharing the data outside the device [4]. For SA diagnosis, PSG test is needed, which produces electrical energy signals from sensor devices attached to the human body. The process of sleep monitoring people with SA is highly expensive and beds remain limited. Sometimes, a full night or two nights are required for monitoring in a well-equipped sleep laboratory. PSG-recorded values sometimes misguide health professionals, leading to inaccurate diagnosis.

However, monitoring a person's health condition continuously is extremely difficult. Nonetheless, IoMT makes this possible. Although data transfer is performed remotely, its security and privacy are not assured. Moreover, data are sensitive, and a need for authentication technology persists, given that various attacks can enter the IoMT environment through the internet. Some attackers easily acquire control over the medical device remotely. Malware in IoMT greatly affects its communication and control on the medical device. Moreover, traditional techniques are insufficient to highly secure IoMT communication. Recent attacks by Mirai botnets create distributed denial of service due to insecurity in the Internet of Things (IoT) environment. Hence, a strong security technique to detect attacks in the sensitive IoMT environment is warranted [5–7].

This research contributes security features as follows:

1. Sleep apnea is monitored using health sensors, such as an oximeter, and stress is monitored on the basis of the heart rate. Data are collected and transmitted to fog nodes using the IoMT framework.

2. IoMT uses forward neural network to train the features and uses KNN to classify SA accurately. The classified data is stored in fog nodes using a signature encryption technique.

The rest of the article is structured as follows. Section 2 presents the survey on IoMT. Section 3 demonstrates the proposed architecture and apnea detection using IoMT. Section 4 discusses the result evaluation. Section 5 concludes.

2 Literature Survey

The information or data is connected and communicated through the internet using the IoT. Smart devices of homes, cars, watches, and so on are connected to the internet to transfer real-time data from user to end user. Moreover, IoT produces Wireless Sensor Networks (WSN), smart technologies, cloud

network, and so on [8]. Human to machine communication [9] is abruptly transferred to machine-machine communication. Recently the IoT became promising in smart applications, such as the health industry, smart city, and so on. Thus, this survey focused on intelligent monitoring of SA diagnosis continuously. The Internet of Intelligent Things (IoIT) [10–12] blends the artificial intelligence in the healthcare system to analyze the data logically.

The main disadvantages of using the IoT is limited bandwidth processing, less memory, and small structure, which cause security attacks and privacy threats [13–16]. These factors influence high research interest in IoT security. To address IoT security, various cryptographic frameworks and technology are suggested [17–22]. Especially in the medical system, handling patient data is highly sensitive for the IoT [23,24]. Central cloud server requires high security structure for providing data authentication.

Some studies explored the adaptive architecture for IoMT architecture [25]. This work provides high security for health dataset using public and private key structures. However, the security of the system is not highly adaptive. Thus, this work explores whether the hybrid security system using a cyber security algorithm for the IoMT is implemented [26]. Streaming data is transmitted via nodes using high authentication [27] to secure the IoMT real-time data in networks. Previous research discussed the security of IoMT with different techniques [28].

This study discussed several SA surveys. The novel recurrent neural architecture is used to extract the apnea features from input dataset [29]. Machine learning classifiers, such as the support vector machine (SVM) [30], threshold-based detectors [31], and regression trees with Adaboost are used to classify SA from the input feature set. The health-based smart contracts [32,33] are used for IoMT to transfer health data [34–38].

3 Proposed Methodology

Although SA syndrome is a common disease, patient diagnosis is difficult. Thus, smart monitoring of the sleeping habit of patients is presented. It monitors the variations in stress and observes the patient's heart rate and the blood oxygen level while asleep. The architecture of SA syndrome analysis is presented in Fig. 1. The sensor transmits the values to the data analysis section. Here, SA is analyzed on the basis of the input SpO2 value. The forward neural network and KNN classifier is used to detect SA in patients.

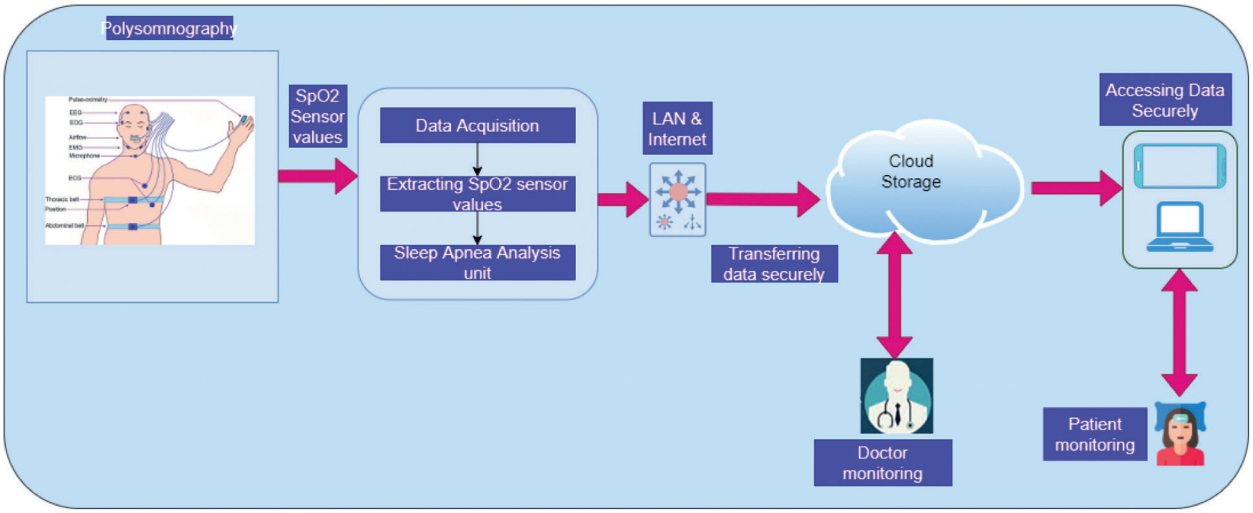

Figure 1: Sleep apnea syndrome analysis

3.1 Visualizing of Sleep Disorder

During sleep state, the nervous system becomes inactive, and the relaxation of muscles forces the eyes to close. It is also associated with low movement, stress less posture, and consciousness becomes suspended involuntarily. To monitor the sleep disorder, patients must undergo five stages, which include rapid eye movement (REM) and non rapid eye movement (NREM). Fig. 2 shows the detailed sleeping stages categorically.

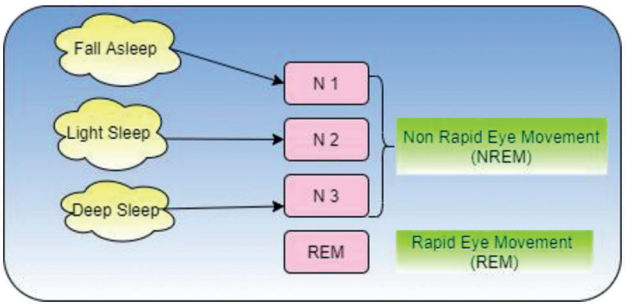

Figure 2: Categorized sleep stages

Human beings have five stages of sleep. Stages 1 and 2 are considered light sleep in which people can be easily awakened. Stage 3 is the deep sleep, Stage 4 represents very deep sleep, and Stage 5 is the REM. Each stage requires 5–15 minutes to complete. After completion of five stages, it starts again from Stage 1. On average, 90 to 110 minutes are needed to complete a sleep cycle. Any irregularity that occurs within the five sleep stages is a sleep disorder. Thus, to maintain a good sound sleep, sufficient sleep in each stage and sleep cycle must be obtained. Fig. 2 presents the sleep stages.

3.2 Monitoring Sleep Apnea

During the sleep state, some breathing-related disorder occurred is called SA. As shown in Fig. 3 for monitoring SA, SpO2 and heart rate variability(HRV) sensor devices are attached in various organs in the body. Electrical energy emitted by the body is collected from these sensors and transmitted as graphical representation and stored in the fog computing network. This procedure is the Polysomnogram diagnosis.

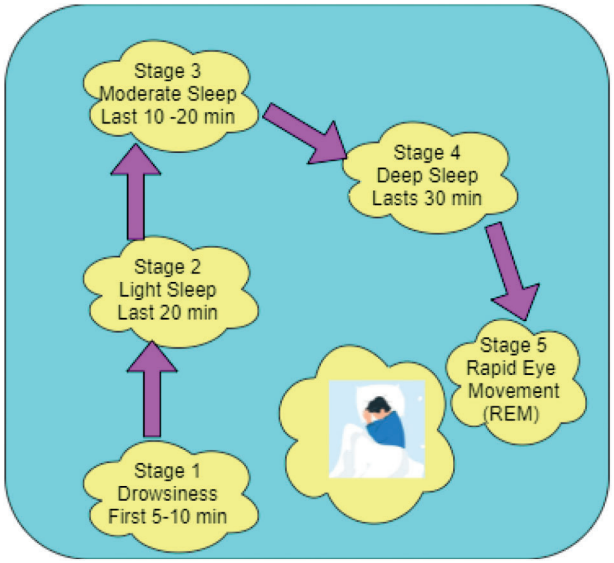

Figure 3: Sleep stages

3.3 Proposed - IoMT-Fog Computing

IoMT sensor values, such as the heart rate, and oximetric values are collected and stored in the fog computing-based network. Fig. 4 shows the IoMT with the fog computing process. Fig. 4 contains two layers, namely, the IoMT section and the fog computing layer. In the IoMT layer, data are collected from sensor devices and are classified into sensitive data (confidential data) and non-sensitive data (non-confidential data). This classified data is transferred to the fog layer, which contains fog servers. Then, data encryption and authorization are performed by a hashing technique of Advanced Signature-Based Encryption (ASE) of Diffie-Hellman key exchange and digital signature. This algorithm is used to exchange information between IoMT devices securely.

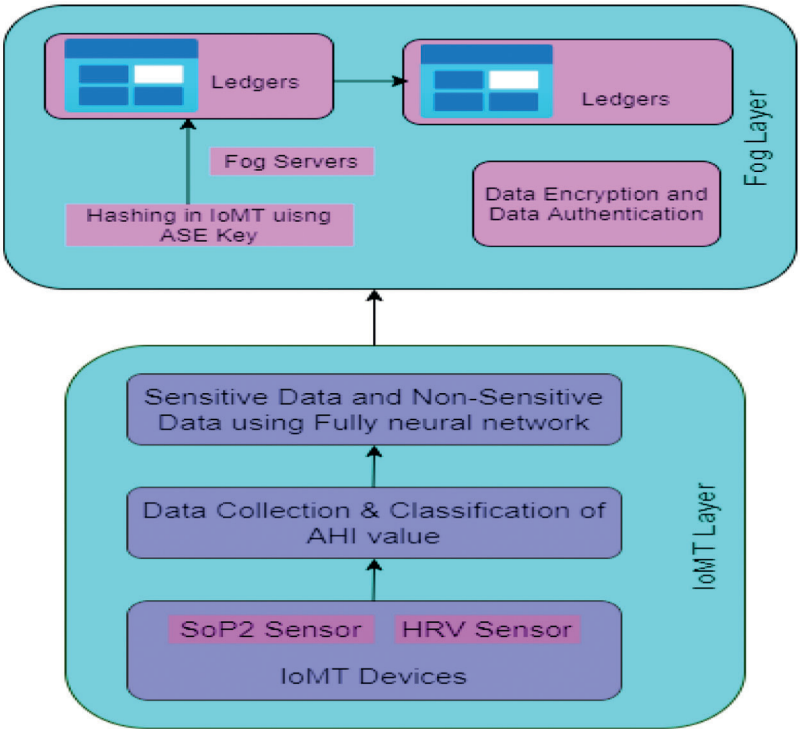

Figure 4: IoMT with fog computing

3.3.1 IoMT Layer

The IoMT layer contains wearable sensor devices of SpO2, which extract the electrical energy signal of SpO2 and HRV. This combination of SpO2 levels and HRV is used to reduce the false detective cases and increases accuracy. This work implementation is focused on monitoring heart rate and oxygen blood level when SA transpires in the sleep state of a patient. When SA happens to the patient, the system will alarm the doctor and observe the readings stored in the fog node securely. The Apnea-Hypopnea Index (AHI) is used to measure SA severity. Tab. 1 displays the AHI value.

$$AHI = \frac{\text{Total no. of Apnea Events} + \text{Total no. of Hypopnea Events}}{\text{Actual Sleep Time}} \times 60 \quad (1)$$

Algorithm 1 represents the patient's SA severity.

Table 1: Sleep apnea severity by AHI value

AHI value	Ratings
<5	Normal (No sleep apnea)
5 to 15	Mild sleep apnea
15 to 30	Moderate sleep apnea
>30	Severe sleep apnea

Algorithm 1: Classification of data on the basis of the AHI value

Input: Monitor and collect the electrical energy signals of SpO2 and HRV.

Output: Analyze the sleep apnea level during sleep.

Step 1: Read the total number of apnea and hypopnea events

Step 2: Calculate AHI using Eq. (1).

Step 3: Read AHI value from Tab. 2

Step 4: If $AHI \leq 5$ then display "Normal"

Step 5: If $(5 < AHI \leq 15)$ then display "Mild Sleep"

Step 6: If $(15 < AHI \leq 30)$ then display "Moderate Sleep"

Step 7: If $(AHI \geq 15)$ then display "Severe Sleep"

Step 8: End.

Step 9: End.

Step 10: End.

Step 11: End.

In the IoMT layer, data are collected and classified on the basis of the AHI value. The data are classified as sensitive information and non-sensitive information using FCNN and k-nearest neighbour (k-NN) classifier. Fig. 5 shows the FCNN diagram for SA classification.

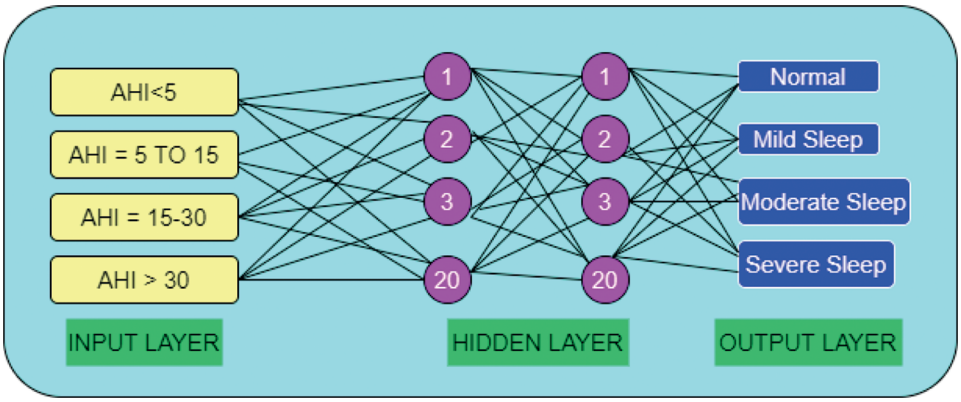

Figure 5: FCNN of SA

This FCNN has one input layer, two hidden layers, and one output layer with 20 neurons. This model is used to develop a relationship between AHI value and sleep stages. To obtain accurate classification after applying FCNN, KNN is implemented. In the KNN classification, the input value is the k-nearest neighbor, and the output value assigns the feature vector class membership. In the classification of KNN, Euclidean distance metric measures are used,

$$Euclidis(x,y) = \sqrt{\sum_{i=1}^{n}(y_i - x_i)^2} = \sqrt{(y_1 - x_1)^2 + (y_2 - x_2)^2 + \ldots + (y_n - x_n)^2}. \quad (2)$$

In Eq. (2), classification is done by the majority votes of neighbourhood values that are grouped together. Here the value of k should be assigned only an odd number. That is, 1-NN, 3-NN, 5NN, and so on.

3.3.2 Fog Layer

In the fog layer, the classification of data is stored for promoting accuracy, security, and scalability. Fog servers are used to generate data encryption and decryption using Diffie-Hellman encryption in the fog node. Algorithms 2 and 3 are used to encrypt and decrypt the information.

Symbolic Notation
$patient_{psg}$: *Sleep Apnea patient*
dr_i : *Doctors*
psg_IoMT : *IoMT devices*
$psg - data$: *Sleep Apnea patient's data*

Algorithm 2: Reading data from IoMT devices to Fog Node

Input: Patients with SA = ($patient_{psg1}$, $patient_{psg2}$, $patient_{psgn}$, . . . , $patient_{psgn}$)

Doctors: (dr_1 , dr_2 , dr_3 , . . . , dr_n)

IoMT devices: (psg_IoMT_1, psg_IoMT_2, ..psg_IoMT_n)

Output: SA patient's PSG data

While $patient_{psg}$ in $Patient_{list}$**do**

Select $patient_{psg}$

For each *psg_IoMT* **do**

IF doctor dr_i choose *psg_IoMT* **then**

Retrieve $PSG(patient_{psg}, psg\_IoMT)$

Store in the fog network

End

End

End

Algorithm 1 retrieves data from IoMT devices and transfers to fog nodes. In the fog node data from sensor devices of SoP2, HRV are stored securely. Algorithm 2 describes the data encryption and decryption using the Diffie-Hellman encryption during fog computation. ASE algorithm comprises asymmetric cryptographic operations, such as the Diffie-Hellman key exchange and digital signature.

Symbolic Notation
$psg - Polysomnography - data$
$symmk - Symmetric\ Key$
$publk - public\ key$
$cit - cipher\ text$
$cikey - cipher\ key$
$spublk - signed\ public\ key$
$sprivk - signed\ private\ key$
$IoMTpsg - Polysomnography\ data\ generated\ from\ IoMT\ devices$
$symm\_encrypt - Symmetric\ encryption$
$asymm\_encrypt - aSymmetric\ encryption$
$psgsign - signature\ of\ the\ patient$
$privkey - Receiver's\ private\ key$
$pubkey - Receiver's\ public\ key$

Algorithm 3: Diffie-Hellman Encryption in the Fog Node

Function *Encryption DHEB* $(IoMTpsg)$

If the SA patient confirms *psg* store in fog node then

Generate key of symmetric *symmk*

$cit \leftarrow symm\_encrypt(IoMTpsg, symmk)$

$cikey \leftarrow asymm\_encrypt(symmk, publk)$

Else

Do nothing

End if

End function

Function $psgsign(IoMTpsg)$

If the SA patient selects confidential data from the fog node then

Generate asymmetric key pair $(spublk,\ sprivk)$

Generate digital signature using *sprivk*

Share *spublk* to the receiver

End if

End function

Algorithms 3 and 4 typically perform the encryption and decryption of the SA patient's data by using the digital signature of hash, and private key produces the Diffie-Hellman method for the exchange of the key among various mobile IoMT devices and fog nodes.

Algorithm 4: Diffie-Hellman Decryption in the Fog Node

Function Decryption DHEB$(cit, cikey, symmk)$

$symmk \leftarrow decryption\_asymmk(cikey)$

$IoMTphr \leftarrow decryption(cit, symmk)$

End Function

4 Results and Analysis

Independent analysis of SA is a breathing disorder that occurs during a person's sleep state. In this work, FCNN-KNN+ASE uses two public datasets of Sleep-EDF-2013 and Sleep-EDF-2018. For evaluation, a 20-fold cross validation was applied to all 250 PSG data values of the dataset. The sleeping stages of R & K standard of W, N1, N2, N3, N4, and REM are used to evaluate FCNN-KNN+ASE. The parametric measures are given below.

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{3}$$

$$precision = \frac{TP}{TP + FP} \tag{4}$$

$$recall = \frac{TP}{TP + FN} \tag{5}$$

$$F1 - Score = \frac{2 * precision * recall}{precision + recall} \tag{6}$$

$$Kappa = \frac{accuracy - P_e}{1 - P_e} \tag{7}$$

$$MF1 = \sum_{i=1}^{10} \frac{F1 - score_i}{5} \tag{8}$$

$$MAE = \frac{1}{N} \sum_{i=1}^{n} |\propto_i - \propto_i^{'}| \tag{9}$$

$$RMSE = \sqrt{\frac{1}{n} \sum_{i=1}^{n} |\propto_i - \propto_i^{'}|} \tag{10}$$

where TP-True Positive, TN-True Negative, FP-False Positive, FN-False Negative, and P_e is Hypothetical probability. Tabs. 2 and 3 shows that confusion matrix of Sleep-EDF-2013 dataset in FCNN-KNN+ASE using 20-fold cross-validation.

Tab. 4 shows the comparison of our proposed work with other machine learning algorithms in the parametric metric measures of kappa and MF1 score values using two different datasets of Sleep-EDF-2013 and Sleep-EDF-2018.

Table 2: Confusion matrix of the leep-EDF-2013 dataset using 20-fold cross validation

	W	N1	N2	N3	REM	Precision %	Recall%	F1-Score%
W	7521	600	198	19	265	91.6	85.9	89.8
N1	475	1179	685	14	578	54.9	41.4	47.8
N2	110	292	16340	726	875	86.9	89.2	89.1
N3	7	3	821	4821	15	87.2	86.1	85.9
REM	75	154	598	1	6945	80.4	90.1	85.2

Table 3: Confusion matrix of the sleep-EDF-2018 dataset using 20-fold cross-validation

	W	N1	N2	N3	REM	Precision %	Recall %	F1-Score%
W	61256	3278	377	16	589	91.8	92.9	91.8
N1	4181	9485	5668	141	1827	51.8	43.8	48.9
N2	612	3567	57891	3087	2521	84.2	86.7	85.2
N3	45	29	3225	9356	35	74.2	74.1	73.2
REM	880	1680	2013	78	21895	81.3	83.2	81.8

Table 4: Comparison of sleep-EDF-2013 and sleep-EDF-2018 datasets

	Sleep-EDF-2013 dataset		Sleep-EDF-2018 dataset	
Algorithm	**Kappa**	**Melt Flow Index (MFI) (%)**	**Kappa**	**MFI (%)**
FCNN-ASE	0.76	79.34	0.79	81.12
KNN-ASE	0.72	75.12	0.76	78.45
FCNN-KNN +ASE	0.7	81.37	0.8	84.65

Tab. 5 unveils that the evaluation of FCNN-KNN+ASE was compared with FCNN-ASE and KNN-ASE. Our proposed work obtained better value in kappa of 0.7 in the Sleep-EDF-2013 dataset and obtained a kappa value of 0.8 in the Sleep-EDF-2018 dataset. Similarly, for the MF1 score value of the Sleep-EDF-2013 dataset obtained 81.37% and the Sleep-EDF-2018 dataset obtained 84.65% in our proposed work, FCNN-KNN+ASE. Tabs. 6 and 7 show the calculating error rate of the Sleep-EDF-2013 and Sleep-EDF-2018 datasets.

Table 5: Error rate for the sleep-EDF-2013 dataset

Algorithm	Training data		Testing data	
	RMSE	**MAE**	**RMSE**	**MAE**
FCNN-ASE	0.336	0.387	0.323	0.265
KNN-ASE	0.310	0.292	0.245	0.145
FCNN-KNN +ASE	0.016	0.036	0.018	0.012

Table 6: Error rate for the sleep-EDF-2018 dataset

Algorithm	Training data		Testing data	
	RMSE	**MAE**	**RMSE**	**MAE**
FCNN-ASE	0.386	0.387	0.323	0.265
KNN-ASE	0.310	0.292	0.245	0.145
FCNN-KNN +ASE	0.016	0.036	0.018	0.012

Table 7: Communication cost and storage cost in the sleep-EDF-2013 dataset

Algorithm	Communication cost (bits)	Storage cost (bits)
FCNN-ASE	5620	7350
KNN-ASE	4570	3275
FCNN-KNN +ASE (Proposed)	2380	1350

Tabs. 6 and 7 present tthat the error rate for our proposed work produces minimum error rate using two different datasets. Tabs. 8 and 9 unveil that cost of communication and storage cost in bits of different algorithm with two different datasets are given.

Table 8: Communication cost and storage cost in the sleep-EDF-2018 dataset

Algorithm	Communication cost (bits)	Storage cost (bits)
FCNN-ASE	5820	7550
KNN-ASE	4790	3450
FCNN-KNN +ASE (Proposed)	2180	1250

Table 9: Encryption time analysis (ms) in the sleep-EDF-2013 dataset

File Size (MB)	FCNN-ASE	KNN-ASE	FCNN-KNN +ASE (Proposed)
5	13560	13270	12890
10	16350	15750	14780
20	19750	18890	15570
40	21450	20870	17670
100	33890	22450	21350

Tab. 8 demonstrates that our proposed technique obtains minimum communication cost and storage cost compared with other techniques.

Tab. 9 presents that our proposed technique obtains minimum communication cost and storage cost compared with other techniques. Tabs. 9 and 10 reveal that time analysis for encryption of PSG information with various file sizes and stored it in fog-node.

Table 10: Encryption time analysis (ms) in the sleep-EDF-2018 dataset

File Size (MB)	FCNN-ASE	KNN-ASE	FCNN-KNN +ASE
5	13150	13350	12650
10	16550	15890	14250
20	19950	18450	15870
40	21650	20210	17770
100	34250	22350	21130

Tab. 10 shows that our proposed work obtained minimum time analysis for encryption using the Sleep-EDF-2013 dataset and the PSG information, which are collected from SoP2 and HRV sensor devices for diagnosis of SAS.

Tab. 10 demonstrates that our proposed work obtained minimum time analysis for encryption using the Sleep-EDF-2018 dataset and the PSG information, which are collected from SoP2 and HRV sensor devices for SAS diagnosis.

Our proposed work obtained minimum time analysis for decryption using the Sleep-EDF-2018 dataset and the PSG information, which are collected from SoP2 and HRV sensor devices for SAS diagnosis. Fig. 6 shows the average accuracy rate for FCNN-KNN+ASE in the two datasets.

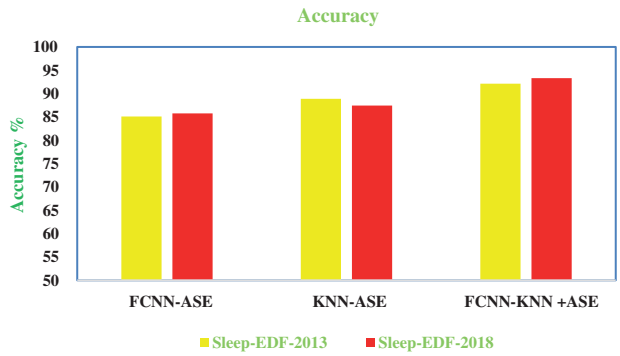

Figure 6: Accuracy

Fig. 6 presents that our proposed work gives high accuracy rate compared with other algorithms. Fig. 7 shows the computation time of our proposed work.

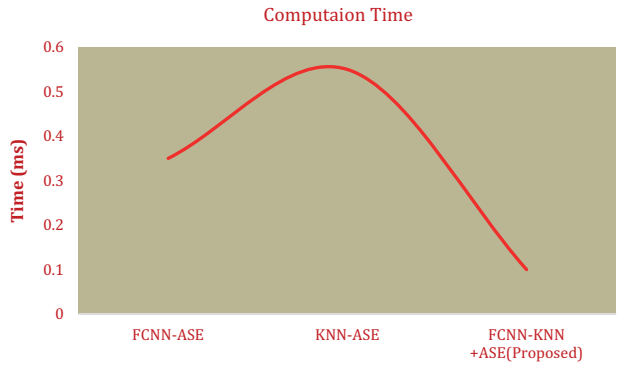

Figure 7: Computation time

The figure shows that the computation of our proposed work obtained minimum time. It produces minimum execution time and minimum error rate.

5 Conclusion

This work provides reference for SA diagnosis using a fog computing-based IoMT in machine learning algorithms. It uses electrical energy signals that are carefully collected from SpO2 and HRV sensor devices and collected data stored in fog computing network. Thereafter, we implement a complex ASE algorithm for encryption and decryption for PSG values, which cannot be accessed by unauthorized users. This work uses two different public datasets of Sleep-EDF-2013and Sleep-EDF-2018. The advantages of the proposed work, FCNN-KNN +ASE, are better security, faster access, minimal time execution, higher accuracy, more flexible, and more reliable compared with other existing algorithms. The overall accuracy performance of this work obtained 92.13% in the Sleep-EDF-2013 dataset and 93.32% in the Sleep-EDF-2018 dataset. Finally, our proposed work analysis provides effective monitoring for diagnosing people with the SA based on PSG values. Future work is upgraded by using various machine learning algorithms with edge computing. Energy efficiency must be calculated in future work to widely enhance fog computing the IoMT.

Acknowledgement: We would like to give special thanks to Taif University Research supporting Project Number (TURSP-2020/98), Taif University, Taif, Saudi Arabia.

Funding Statement: Taif University Researchers Supporting Project Number (TURSP-2020/98), Taif University, Taif, Saudi Arabia.

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

References

[1] R. W. Mcarley, "Neurobiology of REM and NREM sleep," *Sleep Medicine*, vol. 8, no. 4, pp. 302–330, 2017.

[2] S. Chokroverty, "Overview of sleep & sleep disorders," *Indian Journal of Medical Research*, vol. 131, no. 2, pp. 126–140, 2010.

[3] C. Della Monica, S. Johnsen, G. Atzori, J. A. Groeger and J. Dijk, "Rapid eye movement sleep, sleep continuity and slow wave sleep as predictors of cognition, mood and subjective sleep quality in healthy men and women, aged 20-84 years," *Frontiers in Psychiatry*, vol. 9, no. 255, pp. 23–34, 2018.

[4] C. A. Kushida, M. R. Littner, T. Morgenthaler, C. A. Alessi Bailey and J. Coleman, "Practice parameters for the indications for PSG, AASM practice parameters practice parameters for the indications for polysomnography and related procedures: An update for 2005," *Journal of Sleep Research*, vol. 28, no. 4, pp. 24–36, 2005.

[5] Z. Liu, L. Zhang, Q. Ni, J. Chen, J. Wang *et al.,* "An integrated architecture for IoT malware analysis and detection," in *Proc. Int. Conf. on Internet of Things as a Service*, Patna, India, pp. 127–137, 2018.

[6] J. Su, D. V. Vasconcellos, S. Prasad, D. Sgandurra, Y. Feng *et al.,* "Lightweight classification of IoT malware based on image recognition," in *Proc. IEEE 42Nd Annual Computer Software and Applications Conf. (COMPSAC)*, Tokyo, Japan, vol. 2, pp. 664–669, 2018.

[7] V. Clincy and H. Shahriar, "IoT malware analysis," in *Proc. 2018 IEEE 42Nd Annual Computer Software and Applications Conf. (COMPSAC)*, USA, vol. 1, pp. 920–921, 2019.

[8] T. H. Tran and C. Pham, "The internet-of-things based hand gestures using wearable sensors for human machine interaction," in *Proc. 2019 Int. Conf. on Multimedia Analysis and Pattern Recognition (MAPR)*, Hwaseong, Korea, pp. 1–6, 2019.

[9] S. Hu and T. Jiang, "Artificial intelligence technology challenges patent laws," in *Proc. 2019 Int. Conf. on Intelligent Transportation, Big Data & Smart City (ICITBS)*, India, pp. 241–244, 2019.

[10] T. E. Weaver, M. W. Calik, S. S. Farabi, A. M. Fink, M. C. Kapella *et al.,* "Innovative treatments for adults with obstructive sleep apnea," *Nature and Science of Sleep*, vol. 6, no. 137, pp. 1–12, 2014. http://dx.doi.org/10.2147/NSS.

[11] L. Cai, J. Jiang, X. Liu, M. Zhu, K. Cheng *et al.,* "OSA patient monitoring system based on the internet of things framework," in *Proc. 4th Int. Conf. on Smart and Sustainable Technologies (SpliTech)*, India, pp. 1–4, 2019.

[12] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang *et al.,* "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[13] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431–440, 2015.

[14] M. Khomh, F. Haoues, M. Quintero and S. Yacout, "Enforcing security in internet of things frameworks: A systematic literature review," *Internet of Things*, vol. 6, no. 3, pp. 100050, 2019.

[15] J. Ahamed and A. V. Rajan, "Internet of Things (IoT): Application systems and security vulnerabilities," in *Proc. 2016 5th Int. Conf. on Electronic Devices, Systems and Applications (ICEDSA)*, Ras Al Khaimah, United Arab Emirates, pp. 1–5, 2016.

[16] C. Hosmer and M. Dermott, *Defending IoT Infrastructures with the Raspberry Pi*. Germany: Apress, Springer, 2018.

[17] A. Tekeoglu and A. S. Tosun, "An experimental framework for investigating security and privacy of IoT devices," in *Proc. Int. Conf. on Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments*, Vancouver, BC, Canada, pp. 63–83, 2017.

[18] M. Frustaci, P. Pace, G. Aloi and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, 2018.

[19] O. Alrawi, C. Lever, M. Antonakakis and F. Monrose, "Sok: Security evaluation of home-based IOT deployments," in *Proc. Sym. on Security and Privacy (sp)*, San Francisco, CA, USA, pp. 1362–1380, 2019.

[20] M. Chernyshev and H. Peter, "Security assessment of IoT devices: The case of two smart TVs," in *Proc. Conf.: 13th Australian Digital Forensics Conf.*, Australia, 2015.

[21] B. Ali and A. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," *Sensors*, vol. 18, no. 3, pp. 817, 2018.

[22] O. Mazhelis and P. Tyrväinen, "A framework for evaluating internet-of-things platforms: Application provider viewpoint," in *Proc. IEEE World Forum on Internet of Things (WF-IoT)*, Louisiana, USA, pp. 147–152, 2014.

[23] W. Xi and L. Ling, "Research on IoT privacy security risks," in *Proc. Intelligent Technology, Industrial Information Integration (ICIICII)*, Wuhan, China, pp. 259–262, 2016.

[24] S. S. Rani, J. A. Alzubi, S. K. Lakshmanaprabu, D. Gupta and R. Manikandan, "Optimal users based secure data transmission on the internet of healthcare things (IoHT) with lightweight blockciphers," *Multimedia Tools Application*, vol. 18, no. 3, pp. 1–20, 2019.

[25] W. Leister, M. Hamdi, H. Abie, S. Poslad and A. Torjusen, "An evaluation framework for adaptive security for the IoT in ehealth," *International Journal of Information Security*, vol. 7, no. 3, pp. 93–109, 2014.

[26] D. Nkomo and R. Brown, "Hybrid cybersecurity framework for the Internet of medical things (IOMT)," in *Proc. 2019 IEEE 12th Int. Conf. on Global Security, Safety and Sustainability (ICGS3)*, Chennai, India, 2019.

[27] M. A. Jan, M. Usman, X. He and A. U. Rehman, "SAMS: A seamless and authorized multimedia streaming framework for WMSN-based IoMT," *IEEE Internet of Things*, vol. 6, no. 2, pp. 1576–1583, 2019.

[28] M. Usman, M. A. Jan, X. He and J. Chen, "P2DCA: A privacy-preserving based data collection and analysis framework for IoMT applications," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 6, pp. 1222–1230, 2019.

[29] J. Cecil, A. Gupta, M. Pirelacruz and P. Ramanathan, "An IoMT based cyber training framework for orthopedic surgery using next generation Internet technologies," *Informatics in Medicine Unlocked*, vol. 12, no. 3, pp. 128–137, 2018.

[30] S. Liaqat, A. Akhunzada, F. S. Shaikh, A. Giannetsos and M. A. Jan, "SDN orchestration to combat evolving cyber threats in internet of medical things (IoMT)," *Computer Communications*, vol. 160, no. 4, pp. 697–705, 2020.

[31] B. L. Koley and D. Dey, "Real-time adaptive apnea and hypopnea event detection methodology for portable sleep apnea monitoring devices," *IEEE Transactions on Biomedical Engineering*, vol. 60, no. 12, pp. 3354–3363, 2013.

[32] M. Abdel Basset, N. Moustafa, R. Mohamed, O. Elkomy and M. Abouhawwash, "Multi-objective task scheduling approach for fog computing," *IEEE Access*, vol. 9, no. 3, pp. 126988–127009, 2021.

[33] M. Abouhawwash and A. Alessio, "Develop a multi-objective evolutionary algorithm for pet image reconstruction: Concept," *IEEE Transactions on Medical Imaging*, vol. 40, no. 8, pp. 2142–2151, 2021.

[34] B. L. Koley and D. Dey, "Real-time adaptive apnea and hypopnea event detection methodology for portable sleep apnea monitoring devices," *IEEE Transactions on Biomedical Engineering*, vol. 60, no. 12, pp. 3354–3363, 2013.

[35] A. Lakhan, M. A. Mohammed, A. N. Rashid, S. Kadry, S. Panityakul *et al.,* "Smart contract aware ethereum and client- fog-cloud healthcare system," *Sensors*, vol. 21, no. 12, pp. 4093, 2021.

[36] M. Abdel Basset, R. Mohamed, M. Abouhawwash, R. K. Chakrabortty and M. J. Ryan, "EA MSCA: An effective energy aware mult objective modified sine-cosine algorithm for real-time task scheduling in multiprocessor systems: Methods and Analysis," *Expert Systems with Applications*, vol. 173, no. 4, pp. 114699, 2021.

[37] M. Abouhawwash, "Hybrid evolutionary multi-objective optimization algorithm for helping multi-criterion decision makers," *International Journal of Management Science and Engineering Management, Taylor& Francis*, vol. 16, no. 2, pp. 94–106, 2021.

[38] A. Lakhan, M. A. Mohammed, S. Kozlov and J. J. Rodrigues, "Mobile-fog-cloud assisted deep reinforcement learning and blockchain-enable IoMT system for healthcare workflows," *Transactions on Emerging Telecommunications Technologies*, vol. 12, no. 4, pp. e4363, 2021.