Blockchain Technology and Neural Networks for the Internet of Medical Things

Dawid Połap*, Gautam Srivastava†, Alireza Jolfaei‡, Reza M. Parizi§
*Faculty of Applied Mathematics, Silesian University of Technology, Kaszubska 23, 44-100 Gliwice, Poland
†Department of Mathematics and Computer Science, Brandon University, Brandon, MB R7A 6A9, Canada
‡Department of Computer Science, Macquarie University, Australia
§College of Computing and Software Engineering, Kennesaw State University, GA, USA

Email: {Dawid.Polap@polsl.pl, srivastavag@brandonu.ca, alireza.jolfaei@mq.edu.au, rparizi1@kennesaw.edu}

***Abstract*—In today's technological climate, users require fast automation and digitization of results for large amounts of data at record speeds. Especially in the field of medicine, where each patient is often asked to undergo many different examinations within one diagnosis or treatment. Each examination can help in the diagnosis or prediction of further disease progression. Furthermore, all produced data from these examinations must be stored somewhere and available to various medical practitioners for analysis who may be in geographically diverse locations. The current medical climate leans towards remote patient monitoring and AI-assisted diagnosis. To make this possible, medical data should ideally be secured and made accessible to many medical practitioners, which makes them prone to malicious entities. Medical information has inherent value to malicious entities due to its privacy-sensitive nature in a variety of ways. Furthermore, if access to data is distributively made available to AI algorithms (particularly neural networks) for further analysis/diagnosis, the danger to the data may increase (e.g., model poisoning with fake data introduction). In this paper, we propose a federated learning approach that uses decentralized learning with blockchain-based security and a proposition that accompanies that training intelligent systems using distributed and locally-stored data for the use of all patients. Our work in progress hopes to contribute to the latest trend of the Internet of Medical Things security and privacy.**

***Index Terms*—Neural Networks, Federated Learning, Internet of Things, Internet of Medical Things, Blockchain, Patient Data, Security, Privacy.**

I. Introduction

The large leaps forward for technology has led examination practices for the human body to become more accurate. This is important for taking care of our health and also preventing the progression of various diseases. From a technical point of view, the introduction of computing solutions to healthcare has also created various problems. First, the form and place of storing confidential patient data to minimize the likelihood of theft or destruction should be a priority. Moreover, access to data should be provided to medical practitioners for analysis as needed and at the same time block access to those without proper authority. Unfortunately, the mere introduction of the digital circulation of medical data will not make treatment and diagnostics easier in any way and just effects data accessibility. It takes long periods of time sometimes in the weeks for results and analysis of some studies. Not everything is visible to the human eye when it comes to diagnosis. To this end, artificial intelligence (AI) methods can be used to support medical practitioners. Especially in the era of the Internet of Medical Things (IoMT), where devices that perform specific tests can exchange data and process it remotely.

The future of medical systems should include systems that are remotely accessible, wireless in nature, and have low latency as well as high reliability. Even if a wireless device loses Internet connection, the device still needs to be able to make decisions via artificial intelligence (AI), machine learning (ML), and deep learning (DL) models. However, training these algorithms in the field of AI/ML/DL on-device requires large data samples compared to the samples available at each device as well as the need to exchanges data with other devices. In this paper, we consider training each device's local model by exchanging the local data samples without the need for centralization. One key aspect and challenge is that the local data are owned by each specific medical device. Therefore, exchange should keep the raw data private from other devices since most likely these samples will contain private information about patients. To this end, as has been proposed in Google's federated learning (FL) [1], each device can exchange its local model parameters, which is more privacy-preserving compared to sharing all the raw data. In FL, the exchange of data is enabled using a central server that has the ability to aggregate all the local model updates and takes create an average, yielding a global model update. Next, each device can download that global model update, and using it can compute its next local update until the global model training is complete. Unfortunately, such a centralized system as described is still very vulnerable to the malfunction of the central server as well as a central point of failure overall. Therefore, a central architecture may not be an ideal solution, calling for a decentralized FL model to be explored for IoMT. There is also the issue of local model update authenticity. If malicious devices start exchanging inaccurate local model updates, the accuracy of the global model will clearly be unreliable. To combat the above-mentioned issues of centralization and model update inaccuracy, we prescribe here to combine the use of FL with blockchain technology to protect the integrity of DL algorithms using in IoMT.

To resolve the known issues of privacy and security in FL (centralization and fake/malicious local updates injected into aggregation process), in this paper we leverage blockchain technology [2]–[6]. The use of blockchain here will be to ensure that the local data updates that are crucial to the FL aggregation, come from authentic trust devices. Moreover, we can store the local updates as transactions on the blockchain that in the future can be used for off-site experimentation and/or verification of DL algorithm accuracy.

In this paper, we propose a model for storing confidential patients' data using on device facilitated by blockchain technology and federated learning. Moreover, this solution can be easily used to encompass artificial intelligence techniques on IoMT. A described solution was tested in some basic experiments to show the potential future impact.

II. Related Work

Blockchain architecture is increasingly used in practice because of the numerous advantages that are primarily related to decentralization, security, and authorization. It is particularly important to use elliptic curve cryptography as described in [7], where Dinh *et al.* point to the flow of information in blockchain technology and analyze the possibilities of use. In [8], Gordon *et al.* introduce the idea of using such safeguards in health care and outline its advantages and disadvantages. Also available solutions in this area are evaluated and compared what can be seen in [9].

Parallel research is being carried out on classifiers to increase their effectiveness as well reduce training time. In [10], Albahar *et al.* show using a convolutional neural network (CNN) effective classification of skin marks. These types of experiments may not only allow classification but also possible prediction of metastases. The idea of prognosis for pancreatic cancer treatment was described and analyzed by using an artificial neural networks (ANN) in [11] or others types of classifier [12], [13].

Scientists from around the world are trying to combine the advantages of both technologies, which is visible in such works as [14]. Winnick *et al.* proposed a new technique model to obtain the best weights configuration in ANN. As a reward for performing tasks in the chain, the given device received a certain number of points indicating its consumption due to the use of computing power to perform this task. Again in [15], Xu *et al.* described using the crowd-intelligence ecosystem for mobile edge computing by apply blockchain ideas.

Recently, since the proliferation of FL research, we have seen a few pivotal works that focus on FL technology as well as the combination of FL and AI/ML/DL algorithms. McMahan *et al.*, focused on creating a communication efficient learning network using a deep learning network and decentralized data [16]. Focusing more on vehicular networks, Samarakoon *et al.* introduced a distributed FL model that was both high in reliability and low in latency [17]. Since latency is a huge issue for V2V communications, the authors attempted to use FL to reduce those latencies while maintaining reliability. Nishio *et al.* focused their research on choosing clients for FL in mobile computing environments [18]. The results garnered in their work can help networks make better choices on which devices to use for FL. Finally, closely related to our work proposed here, Kim *et al.* proposed methodology for on-device FL via blockchain in their short paper [19]. Apart from Kim *et al.*'s work mentioned in [19], our work in this paper stands alone to date.

Figure 1: X-ray with patient data removed (top right).

III. Proposed Approach

In IoMT, every device is able to download certain, specific data, which can be in the form of a scans and/or examination. However, there is also data whose results are labeled with private information. An example of this is medical photos such as X-rays, where patient data is placed in the corner of the photo. The solution we propose for this type of private information that is often included in various types of medical tests, is to first remove the private information by applying a black rectangle in its place in the actual test. This type of action can be performed at device level itself and an example of it can be seen in Fig. 1 in the top right corner. The type information from each test that is usually recorded in the form can be described as *(data, examination type, results, first name, second name)* and may contain other info sensitive in nature. To protect them, upon removing the sensitive data from the medical test, we store this data in the form of a transaction using blockchain technology.

Let us assume that the examination results will be placed in a database for this type of information. Each record addition generates a unique number id_k ($k \in \{0, 1, \ldots\}$) in the range of the database. For many different devices/examination, there will be many databases, each of which will be marked with id_l ($l \in \{0, 1, \ldots\}$). Adding a new record to the specified database returns the key (id_l, id_k). Then there are data items as $\{$*data, first name, second name, id_l, id_k*$\}$. In the case of patients name, this data can be placed in database containing only these two strings and id_n ($n \in \{0, 1, \ldots\}$), so then, there will be $\{$*data, id_n, id_l, id_k*$\}$. Using this set of numbers, all data put in another database can be obtained, but there is still no security for this, so after making some examination, and adding these results to the respective databases, a transaction can be created using the above information.

Having this set of data in the form of a transaction, a device sends a transaction to the blockchain using $SHA-512$, in

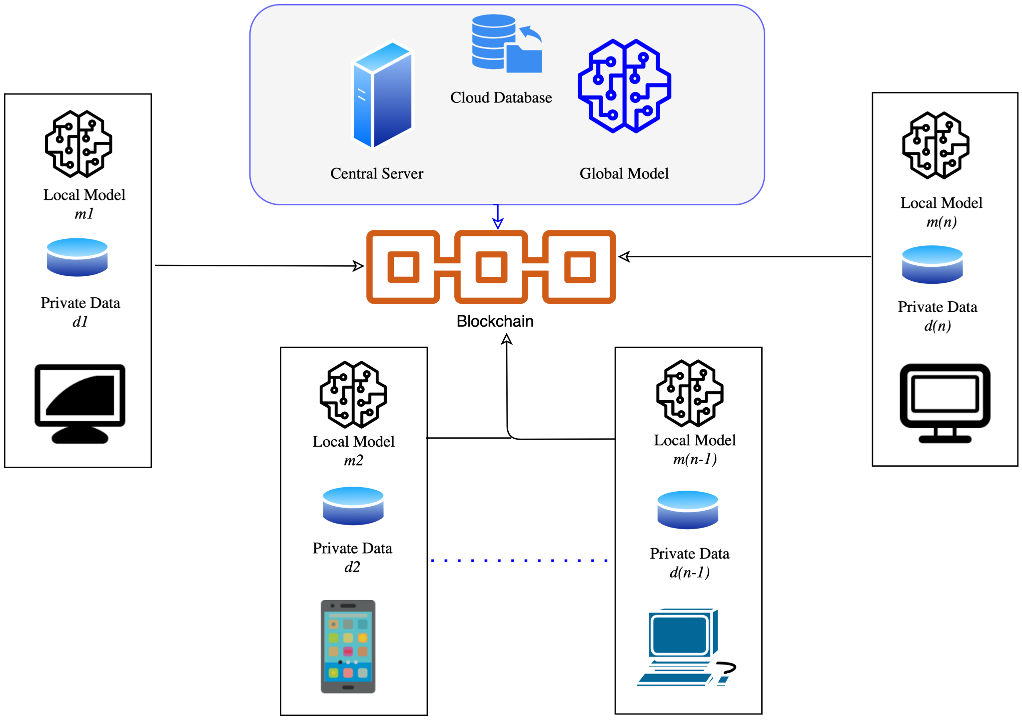

Figure 2: Architecture Overview

64-bits words. Hashed information is supplemented in such a way that the length is 1024 bits or a multiple thereof. In the next step, the message is divided into blocks of 1024 bits and marked as $M^{(1)}$, $M^{(2)}$,..., $M^{(N)}$. Having blocks created in this way, we assume that the initial hash value is known and marked as $H^{(N)}$, which allows to perform the following action

$$H^{(i)} = H^{(i-1)} + C_{M^{(i)}}\left(H^{(i-1)}\right) \mod 2^{64}, \quad (1)$$

where C is understood as a compression function.

An overview of system architecture is illustrated in Figure 2. The architecture is designed within the federated learning framework and is divided into several parts including the global model (i.e., the pre-built machine learning model offered by a medical centre or a company), local model (i.e., the model that is trained on a given local medical device with computing power), IoT medical devices, and the blockchain. The learning is considered as an iterative process where in each iteration the central model is improved. First, the global model is shared with the clients. Second, the initial models at the client level (called local models) are trained with individuals training data–removing the need for sending actual data to the server. Lastly, local models are trained at the client level, and updates (parameters of the model) are stored in the blockchain in the forms of transactions. The central server in order to aggregate and train the global will read the parameters from the blockchain. The global model is updated and the improved model is shared among the individual clients for the next iteration.

In this architecture, the blockchain network could consist of globally participating nodes (i.e., authorized entities) that participate in the verification of transactions. The choice of consensus mechanism and the participating nodes are domain-specific and somewhat technology-dependent and are not discussed here.

A. *System operation in Internet of Medical Things*

Proposed architecture is very flexible for medical devices and different intelligent approach. The AI component learns from all samples all the time, i.e. when $10 \cdot n$ $(n \in \{1, 2, \ldots\})$ subsequent, described samples are added into the database, all data are used in the training process. Hence the requirement to use two of the same AI architectures, where one of them will be used for immediate analysis of new data, and the other for continuous training. If the post-training effectiveness is greater than before, then in the second architecture, the balance configuration is overwritten.

The above mentioned ideas of two the same classifier is stored on local machines, where the basic architecture with weights and parameters of classifier is download from global model. In the case, when accuracy of local classifier is higher than global one more than 1%, the current configuration is used in the global override. Global overwrite causes all locales also to benefit from this change by overwriting theirs.

IV. Machine Learning as a Component of Continuous Data Processing

Databases and protection of user data through the use of blockchain gives access to medical results id_l. Their security can be achieved using additional encryption or key security. Data in the database has confidential information removed, but it is important to include additional fields for the classification of data by disease. At the initial stage of creating such a structure, the data should be supplemented with a diagnosis by medical practitioners. However, at a later stage, artificial intelligence methods (hereinafter referred to as the expert system) should analyze and evaluate this data.

An expert system can perform two basic actions, which are the analysis of new data and the prediction of further disease based on other data. The physician performing the medical tests places the results in an external database. The system, when attaching data, performs analysis using artificial intelligence methods and returns the results to the doctor. Depending on his decision, the results are modified or not and added to the database. This suggests an additional physician support analysis. Also, continuous expansion of knowledge with various data from many patients allows for additional advantages. The first is to improve the operation of methods at individual stages of data analysis. It is worth noting that artificial intelligence techniques are called the data-hungry algorithm, which becomes much more efficient and accurate with a huge amount of data. The second point is the possibility of predicting the development of the disease by existing records.

Performing any medical examination results in the analysis of this data depending on the form of recording this information. In the case of image, the analysis will be based on the use of a convolution network network[20], and for the numerical values, it will be a classic neural network [21], support vector machine [22] or others. In our proposition, we use only image data like x-rays, so in this case, our classifier will be a convolutional neural network.

A convolutional neural network is a type of classifier inspired by the idea of how the brain cortex process images. In the mathematical model, there are three types of layers. The first of them is called convolutional, which is understood as an application of filter on the image. Filter is defined as a matrix of size $k \times k$ and all values of it are searched during training. This type of layer has one purpose - find features of image, so image after this layer, will be called a feature map. The next type of layer is pooling one, which reduces the size of the image using some function like maximum. In that case, for each matrix of pixels, the highest value is transferred into the next layer. These two types of layers can be used more than one. The last type of layer is fully-connected and it is a classic architecture of the neural network. All pixels from last, pooling layer are flattened into vector and passed into fully-connected one. In this layer, are neurons which are calculating activation impulse and pass it forward as defined

$$f\left(\sum_{i=0}^{k}\sum_{j=0}^{k} w_{i,j} \cdot a_{x+i,y+j}\right), \tag{2}$$

where f is an activation function for neuron $a_{x,y}$ where (x, y) means its position. All neurons are connected by synapses. Each of these synapses are buried with weights w_{ij}. These values are modified in the training process to find the best configurations of these values for defined problems.

Training of such a structure is based on modification weights, and for that Adam optimizer can be used. Weights are modified in each iteration t and try to reduce loss function. In this algorithm, statistical values as mean m and variation v with distribution β_1 and β_2 are defined as

$$m_t = \beta_1 m_{t-1} + (1 - \beta_1) g_t, \tag{3}$$

$$v_t = \beta_2 v_{t-1} + (1 - \beta_2) g_t^2. \tag{4}$$

After calculating this two values, they are used in calculation of correlation

$$\hat{m}_t = \frac{m_t}{1 - \beta_1^t} \tag{5}$$

$$\hat{v}_t = \frac{v_t}{1 - \beta_2^t}. \tag{6}$$

This correlation are used in formulas for changing weights in neural network as

$$w_{t+1} = w_t - \frac{\eta}{\sqrt{\hat{v}_t} + \epsilon}\hat{m}_t, \tag{7}$$

where η is understood as learning rate and ϵ 0 is a value to prevent division by zero.

The classifier will return the decision on the patient's condition to the doctor. Based on the received information and his knowledge, the doctor labels the data. The labeled results are added to the database. If such a user does not exist, it is added with the new identifier. Otherwise, the data will be added to the database, but this forces the execution of disease prediction. The prediction consists of collecting all information about the patient and performing additional calculations using artificial intelligence methods depending on the form of the data. All information is used for re-analysis. The module mainly takes into account the date of the test. Each classification returns numerical values from the range $\langle 0, 1\rangle$ for each input file. The obtained results are compared as follows for each two photos from different times

$$k = i_1 - i_2 = \begin{pmatrix} r_1^{i_1} \\ r_2^{i_1} \\ \dots \\ r_n^{i_1} \end{pmatrix} - \begin{pmatrix} r_1^{i_2} \\ r_2^{i_2} \\ \dots \\ r_n^{i_2} \end{pmatrix} = \begin{pmatrix} r_1^{i_1} - r_1^{i_2} \\ r_2^{i_1} - r_2^{i_2} \\ \dots \\ r_n^{i_1} - r_n^{i_2} \end{pmatrix}, \tag{8}$$

where i_1 and i_2 mean two different image results (i_1 is earlier than i_2) and values r are understood as output values for individual classes. Then, these values are analyzed against the results obtained by detecting the largest anomalies. The results can be presented as a set of matrices $\{k^1, k^2, \dots, k^m\}$. The maximum value is then found on each row, which allows the following matrix to be constructed

$$\begin{pmatrix} \max\left(k_{11}^1, k_{11}^2, \dots, k_{11}^m\right) \\ \max\left(k_{21}^1, k_{21}^2, \dots, k_{21}^m\right) \\ \dots \\ \max\left(k_{n1}^1, k_{n1}^2, \dots, k_{n1}^m\right) \end{pmatrix}. \tag{9}$$

If the above values are large, they indicate changes in time, which can be understood as progressive action on a given class.

The same operation can be performed for numerical values. For both classes, and maintaining the structure of classifying classes, the analysis can be performed jointly for both types of data.

V. Experiments

In conducted experiments, we analyze the impact of federated learning with convolutional neural networks. The basic architecture of the described solution in this paper was composed of one global architecture and two local ones. In the beginning, the database was filled up with 110 images of Tuberculosis Chest X-ray Image Data Sets [23], which originally contains 139 images.

Research began with the selection of a global classifier architecture. For this purpose, transfer learning was used using classic architectures such as VGG16, VGG19, Inception, and AlexNet. Each classifier was overtrained with 20 or 40 iterations with a new medical database composed of 50, 70, 90 and 110 photos. Images were split into two sets in ratio of $0.7 : 0.3$ (training: validation). Effectiveness of training sets using 50, 70, 90 and 110 images are presented in Tab. I-II. For each of the selected network configurations, the effectiveness increases as the amount of training data increases.

Architecture	Effectiveness			
	50	70	90	110
VGG16	30%	34%	38%	52%
VGG19	37%	43%	58%	64%
Inception	45%	48%	49%	72%
AlexNet	34%	35%	38%	42%

Table I: The dependence of the classifier's effectiveness on the number of samples in the training set for 20 training iterations.

Architecture	Effectiveness			
	50	70	90	110
VGG16	34%	36%	43%	55%
VGG19	38%	41%	47%	65%
Inception	49%	53%	54%	58%
AlexNet	37%	38%	40%	44%

Table II: The dependence of the classifier's effectiveness on the number of samples in the training set for 40 training iterations.

The best result was achieved by the Inception model trained with 110 images by 40 iterations, so it was chosen as a global model. Then, two local models were created by copying the global architecture. During training, we used 110 images, so 29 was split into two sets containing 15 and 14 images - one set on each local machine. Each of this images were used for recalculating results, and in training one of the local classifier. Training was made two times - by using half and whole set. We notice, that in the case of taking very small number of images as 7 or 8, there is no significant increase of classifier. However, by using whole sets, the accuracy was increased by 1.2% and 1.7%. And in both cases, the global model should be overwritten - but the model with higher

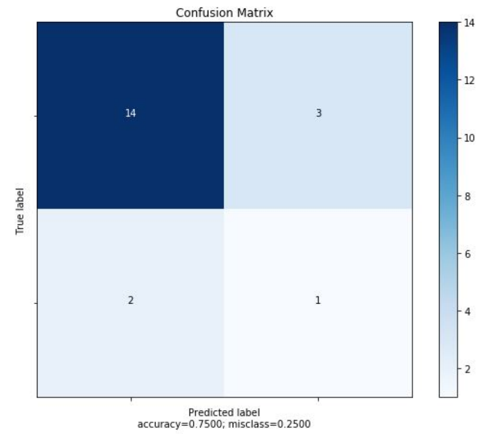

Figure 3: Confusion matrix for conducted experiments regarding comparisons of tests performed at different times.

accuracy was better. This proves, that having some new, private samples can increase the accuracy of classifier and be used by other machines thanks to federated learning approach. The main advantage is the fact that overtraining classifier using private data and sharing only architectural parameters allows not only for higher security but also to increase the accuracy of classifiers.

Moreover, we proposed in Eq. (8) simply comparison data from selected patients. Medical data were marked with three classes – no disease, suspected disease, disease. Hence, the classifier's output was three neurons. To analyze this solution, three images were assigned to 20 people and tested with this solution using CNN with the Inception model trained to achieve effectiveness average 73,7%. The test results were counted and presented as a confusion matrix in Fig. 3. The described solution reached accuracy at level 75%, were in 3 cases, comparison results from classifier were different than the true one. In a real application, this level of accuracy is very low, however, it must be noted that used database in both situations - in training classifier and comparison experiments were very small and limited. And even that, the result is very promising at this stage of our research.

VI. Conclusion

In this paper, we propose an architecture for combining blockchain advantages and artificial intelligence techniques within the privacy-preserving federated learning framework for using the Internet of Medical Things. The described idea was based on protecting training-specific data in the blockchain, and putting new ways of handing machine learning out there from where artificial intelligence can take data for training. In this way, there is a continuous mode of learning and improving classifiers as well as protection for the data itself.

The proposed solution has been tested using medical images data. All initial experiments proofed the advantages of using this architecture by improving the effectiveness of used convolutional neural networks. The main conclusions from conducted experiments are the great possibilities of retraining classifiers on local machines with sharing only parameters of classifier, not private data that was proved by simple simulation tests.

However, conducted experiments were at the very start. In the future, we want to expand our idea to use other classifiers, different data types and analyze the possibility of using these approaches in industrial applications.

REFERENCES

[1] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 10, no. 2, pp. 1–19, 2019.

[2] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K. R. Choo, and M. Aledhari, "Decentralized authentication of distributed patients in hospital networks using blockchain," *IEEE Journal of Biomedical and Health Informatics*, pp. 1–1, 2020.

[3] G. Srivastava, R. M. Parizi, and A. Dehghantanha, "The future of blockchain technology in healthcare internet of things security," in *Blockchain Cybersecurity, Trust and Privacy*. Springer International Publishing, 2020, pp. 161–184.

[4] G. Srivastava, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo, "Data sharing and privacy for patient iot devices using blockchain," in *Smart City and Informatization*. Springer Singapore, 2019, pp. 334–348.

[5] M. Baza, N. Lasla, M. Mahmoud, G. Srivastava, and M. Abdallah, "B-ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain," *IEEE Transactions on Network Science and Engineering*, 2019.

[6] M. Baza, M. Mahmoud, G. Srivastava, W. Alasmary, and M. Younis, "A light blockchain-powered privacy-preserving organization scheme for ride sharing services," *Proc. of the IEEE 91th Vehicular Technology Conference (VTC-Spring), Antwerp, Belgium*, May 2020.

[7] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 7, pp. 1366–1385, 2018.

[8] W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability," *Computational and structural biotechnology journal*, vol. 16, pp. 224–230, 2018.

[9] H. Tang, Y. Shi, and P. Dong, "Public blockchain evaluation using entropy and topsis," *Expert Systems with Applications*, vol. 117, pp. 204–210, 2019.

[10] M. A. Albahar, "Skin lesion classification using convolutional neural network with novel regularizer," *IEEE Access*, vol. 7, pp. 38 306–38 313, 2019.

[11] S. Walczak and V. Velanovich, "Improving prognosis and reducing decision regret for pancreatic cancer treatment using artificial neural networks," *Decision Support Systems*, vol. 106, pp. 110–118, 2018.

[12] H. M. Alshamlan, G. H. Badr, and Y. A. Alohali, "Abc-svm: artificial bee colony and svm method for microarray gene selection and multi class cancer classification," *Int. J. Mach. Learn. Comput*, vol. 6, no. 3, p. 184, 2016.

[13] G. Xu, M. Zhang, H. Zhu, and J. Xu, "A 15-gene signature for prediction of colon cancer recurrence and prognosis based on svm," *Gene*, vol. 604, pp. 33–40, 2017.

[14] A. Winnicka and K. Kesik, "Idea of using blockchain technique for choosing the best configuration of weights in neural networks," *Algorithms*, vol. 12, no. 8, p. 163, 2019.

[15] J. Xu, S. Wang, B. Bhargava, and F. Yang, "A blockchain-enabled trustless crowd-intelligence ecosystem on mobile edge computing," *IEEE Transactions on Industrial Informatics*, 2019.

[16] H. B. McMahan, E. Moore, D. Ramage, S. Hampson *et al.*, "Communication-efficient learning of deep networks from decentralized data," *arXiv preprint arXiv:1602.05629*, 2016.

[17] S. Samarakoon, M. Bennis, W. Saad, and M. Debbah, "Distributed federated learning for ultra-reliable low-latency vehicular communications," *IEEE Transactions on Communications*, 2019.

[18] T. Nishio and R. Yonetani, "Client selection for federated learning with heterogeneous resources in mobile edge," in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE, 2019, pp. 1–7.

[19] H. Kim, J. Park, M. Bennis, and S.-L. Kim, "On-device federated learning via blockchain and its latency analysis," *arXiv preprint arXiv:1808.03949*, 2018.

[20] U. R. Acharya, S. L. Oh, Y. Hagiwara, J. H. Tan, and H. Adeli, "Deep convolutional neural network for the automated detection and diagnosis of seizure using eeg signals," *Computers in biology and medicine*, vol. 100, pp. 270–278, 2018.

[21] G. Villarrubia, J. F. De Paz, P. Chamoso, and F. De la Prieta, "Artificial neural networks used in optimization problems," *Neurocomputing*, vol. 272, pp. 10–16, 2018.

[22] A. Zendehboudi, M. Baseer, and R. Saidur, "Application of support vector machine models for forecasting solar and wind energy resources: A review," *Journal of cleaner production*, vol. 199, pp. 272–285, 2018.

[23] S. Jaeger, S. Candemir, S. Antani, Y.-X. J. Wáng, P.-X. Lu, and G. Thoma, "Two public chest x-ray datasets for computer-aided screening of pulmonary diseases," *Quantitative imaging in medicine and surgery*, vol. 4, no. 6, p. 475, 2014.