International Journal of Data Informatics and Intelligent computing (IJDIIC)
Vol.2, No.1, March 2023, pp. 1~10
DOI: 10.59461/ijdiic.v2i1.42

Using Federated Artificial Intelligence System of Intrusion Detection for IoT Healthcare System Based on Blockchain

Priyanka Tyagi [1], S.K. Manju bargavi [2]
[1]Computer Science and Engineering, School of Engineering and Technology, Sharda University, Noida, India
[2]Department of CS &IT, Jain (Deemed to be University), Bangalore, India

Article Info

Article history:

Received February 22, 2023
Revised March 15, 2023
Accepted March 19, 2023

Keywords:

Blockchain
Internet of things
Edge computing
Intrusion detection systems
Dwarf mongoose optimised
Artificial neural networks

ABSTRACT

Recently Internet of things (IoT)-based healthcare system has expanded significantly, however, they are restricted by the absence of an intrusion detection mechanism (IDS). Modern technologies like blockchain (BC), edge computing (EC), and machine learning (ML) provide a robust security solution that is well-suited to protecting patients' medical information. In this study, we offer an intelligent intrusion detection mechanism FIDANN that protects the confidentiality of medical data by completing the intrusion detection task by utilising Dwarf mongoose-optimized artificial neural networks (DMO-ANN) through a federated learning (FL) technique. In the context of recent developments in blockchain technology, such as the elimination of contaminating attacks and the provision of complete visibility and data integrity over the decentralized system with minimal additional effort. Using the model at the edges secures the cloud from attacks by limiting information from its gateway with less computing time and processing power as FL works with fewer datasets. The findings demonstrate that our suggested models perform better when dealing with the diversity of data produced by IoT devices.

Corresponding Author:

Priyanka Tyagi
Computer Science and Engineering,
School of Engineering and Technology
Sharda University, Noida, India
Email: priyanka.tyagi@sharda.ac.in

1. INTRODUCTION

IoT facilitates the merging of the real world with the data world, making our lives more intelligent and trendy. It accomplishes this by linking the Internet with physical items and exchanging information between them. Smart metering, smart cities, smart healthcare, smart agriculture, and smart transportation are all examples of current prominent IoT applications [1]. The advancement of healthcare is greatly aided by the IoT. Physical devices are a significant and important source of medical data since they use several sensors to continuously monitor vital signs and communicate real-time data with the healthcare staff through the internet [2]. IoT and social networking applications are increasing too rapidly, causing exponential edge data growth. Traditional centralised cloud computing systems provided distant services by centralising data on a server. However, due to network bandwidth restrictions and data privacy concerns, sending all data to the remote cloud in the same way as previously is impracticable and frequently undesirable since it incurs high data transmission costs and doesn't fulfill the demands of certain low-latency applications and services [3]. Edge computing is a new method. Edge-assisted IoT occurs when edge computing moves some network operations and data processing from the core network to the network edge closer to the end user. Edge computing can overcome cloud computing IoT application restrictions. Compared to cloud computing, edge computing provides users

with effective network communication services with reduced latency, more flexible access, and data privacy [4, 5]. On the other side, a distributed, independent, trust-free, and decentralised environment is offered by blockchain technology. Blockchains make advantage of the computing power of all the participating users, resulting in increased efficiency and removing the single point of failure, in contrast to centralised systems, which have issues with node failures, trustworthiness, and privacy [6]. Furthermore, because of its immutable and unchangeable characteristics, blockchain provides improved privacy and data reliability. Blockchain and IoT integration are crucial for computation communication systems [7]. A study [8] proposed blockchain architecture based on users to guarantee the security of data communication in the IoT. Study [9] defines the impact of blockchain technology on smart healthcare, defines the deployment of blockchain technology in healthcare, and ultimately establishes a stakeholder-based advanced application system for smart healthcare. The potential uses of a blockchain-based P2P resource-sharing network were widely analyzed by a study [10]. This paper is a comprehensive resource for learning about the state of the art in smart home network deployment and capabilities, They determined that issues like funding for smart cities and smart home security weren't addressed properly in the research. A review of federated learning strategies, with an emphasis on those applied in biomedicine, was provided by the study [11]. Analyze and discuss the general solutions to the privacy issues, system issues, and statistical obstacles that come with federated learning, with an emphasis on the potential and consequences for healthcare. In the paper [12], a "BDSDT" (Blockchain-orchestrated Deep Learning) solution for Secured Data Transfer in IoT-enabled healthcare systems is proposed. An IDS built on ML-based methods was developed by the study [13]. Two linear projected transformation techniques, namely Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) are used by the underlying scheme to first provide privacy (LDA). The k-nearest neighbours method (k-NN) was utilised to identify and report intrusion using the extracted features. Deep Neural Network (DNN) and stacking AutoEncoder (AE) were employed in Study [14] creation of an IDS for detecting attacks in IoT networks. A privacy-based IDS was suggested by a study [15] to safeguard and secure the data of the smart power network. Long Short-Term Memory (LSTM) is used to identify attacks while the ePoW and Variational AutoEncoder (VAE) techniques are used to offer privacy. DeepChain is a system created by a study [16] that uses blockchain and DL to guarantee the privacy of local gradients. Utilizing a convolution neural network, the IDS was created (CNN). To secure SDN-based industrial applications, paper [17] developed a blockchain- and DL-based deep Boltzmann machine-based security framework. A blockchain consensus mechanism based on votes was implemented to register and authenticate SDN switches. Author [18] suggests a blockchain-based approach in this research to protect E-Health records collected from IoT devices. To address this problem, [9] the suggested blockchain-based system deploys on a private cloud. In this, we suggest a FIDANN that protects the confidentiality of medical data by completing the intrusion detection task by utilising DMO-ANN through an FL technique.

Contribution

The contributions of the paper are included in the list that follows:

- In order to avoid assaults on a healthcare system, we propose a FIDANN model that can function with limited memory and resources at network peripheries. The DMO-ANN was selected because of its benefits, including its ability to work with data from a wide variety of sources and its superior performance in dealing with the diversity of data generated by IoT sensor devices.
- Using federated edge cloud-IDS architecture to avoid centralised issues like data loss and protect local training data for healthcare systems. Applying the detection model at the edge of the system near the attack source speeds detection and minimizes cloud work.
- Combining blockchain technology with Federated Learning way to store localized parameters for upgrading the global model secures the systems against poisoned assaults and gives complete disclosure and data integrity over the decentralized training procedure.

The further part of the portion includes such as part 2 represents the suggested technique, part 3 represents the experimental result and part 4 denotes the concluded part.

Problem statement

IoT devices have minimal memory and computing capability whereas blockchain requires plenty of resources. Blockchain nodes verify transactions by sharing data. IoT end devices have limited bandwidth. Blockchain bandwidth needs may surpass various Edge-device bandwidth limitations. Blockchain technology allows all devices to communicate using pre-defined protocols. Healthcare apps have different requirements and limits. Health data measurement frequency is expected to increase. Storing a lot of patients' health records on the blockchain may be an issue.

2. METHOD

In this study, we propose an intelligent intrusion detection mechanism FIDANN that secures medical data by using DMO-ANN through an FL. A distributed ML framework is FL. Each of FL's several organization has access to data and computational resources. It is specifically made to aggregate local ML models that have been trained on local computing devices with data without sharing information outside of the institutes to create global ML models. "The data does not move, the model moves" is the central principle behind FL. Figure 1 depicts the structure of the suggested methodology.

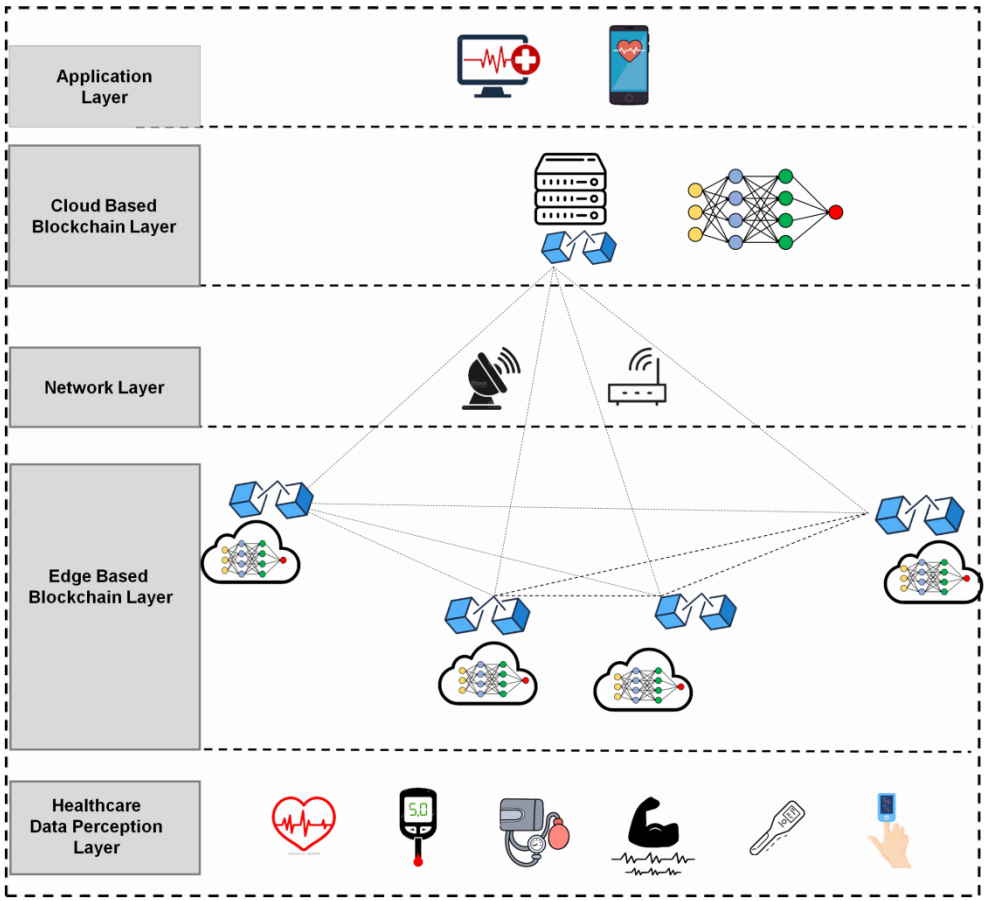

Figure 1. Overview of the suggested methodology

2.1. Data collection

With the recent broad use of EHRs, researchers have cheap and easy access to extensive longitudinal clinical data. Most FL research makes use of EHR data collected from a variety of medical centres. Approximately 40,000 severely sick patients who were hospitalised at the Beth Israel Deaconess Medical Center are represented in the MIMIC59. MIMIC has become the standard set of data for ML research. Since this is the case, researchers in the field of ML may devote their time to assessing approaches with real-world data in order to demonstrate their efficacy. Yet, MIMIC exhibits less-than-ideal features for FL research. MIMIC originates from a unique research institute.

2.2. Edge-based blockchain layer

It is IoT gateways (GW) that form the block chain's edge layer. Each GW contains medically-relevant sensing equipment. Many different protocols for accessing networks were supported by the gateways. The multi-attack detection process must be carried out via an IoT gateway. An IDS was built for the edge server (ES) to standardise data and identify distinct neural network-based assaults. To prevent further damage to the clouds or other resources in the event of a specific assault, the suggested module will be built in the FL model and trained in the edge. As attack resources get closer, the amount of time it takes to spot an infiltration will decrease.

Because the FL model may be applied to smaller data sets, less processing and computation time will be required. Once the modules have been learned, their respective weights will be sent to a blockchain-based distributed ledger and recorded in a linked block that links the GW nodes to the server node in the succeeding cloud tier. These interconnected cubes will be used for summarization and averaging as well. Finally, the chain

is encrypted using a hash function that ties the blocks together within the chain, making it immutable due to the use of consensus methods (smart contracts-SC).

Blockchain-based SC is an automated protocol for executing financial transactions. With the use of SC, participants to transactions can predetermine the conditions under which they will be conducted mechanically. There is a wide range of environments suitable for deploying SC. SC, in other words, permits users to run a script on a blockchain network in a verified way, therefore resolving numerous issues with a minimum of trust. The deterministic protocols and promises provided in an SC enable users to eliminate the requirement for a trusted third party. An SC may be uniquely identified by its address and account on the distributed ledger. As a result, it can operate as an escrow since it can monitor its state and acquire blockchain-based assets. With the help of the network, SC makes available a set of operations that may be initiated by sending the contract a transaction. Each node in the network has access to every SC stored on the blockchain, which means that they can all see the contract's instructions and follow them. We can think of the patient's wearable gadget and the healthcare practitioners as two parties in this scenario that need to rely on the integrity of the blockchain. Additionally, as was previously indicated, patients can give and deny access to their data using other SC.

One of FL's most significant issues, poisoning attacks are addressed by the suggested model. Each ES obtains the updated weight values, encrypts the information gathered, and creates the associated signature using a secret key of its own. Then, ES combines the cypher text and transmits it, together with the signature, to the active blockchain layer administered by an SC, ensuring the confidentiality and validity of the transaction. When an SC receives data from many ESs, it uses the public keys associated with those ESs and the data recorded on the blockchain to determine whether or not the data is valid. In response, the active blockchain may be retrieved by the CPCC, which can then extract the aggregate plain text using its secret key. The connections between the CPCC and ESs, as well as the ES and the appropriate local model, are bidirectional in most IoT edge computing applications. Similar to terminal-based edge computing information storage, the local model may send and receive data with the CPCC using the blockchain network and ES.

2.3. Network layer

In the network layer, this is the component that is accountable for ensuring the security of data transactions moving from lower to higher layers. It is referred to as the connection layer and its primary purpose is to offer route management.

2.4. Cloud-based blockchain layer

To keep the ANN algorithm's global weights up-to-date, the cloud-based BC layer is in charge of averaging out the weights reported by the ESs and recording them in the blockchain ledger. For optimal network security, the cloud periodically distributes the aforementioned modified weights to all gateways, where they are used to update the weights of local models. Figure 2 shows the FIDANN blockchain network. At last, the Application layer is in charge of tracking patient vitals.

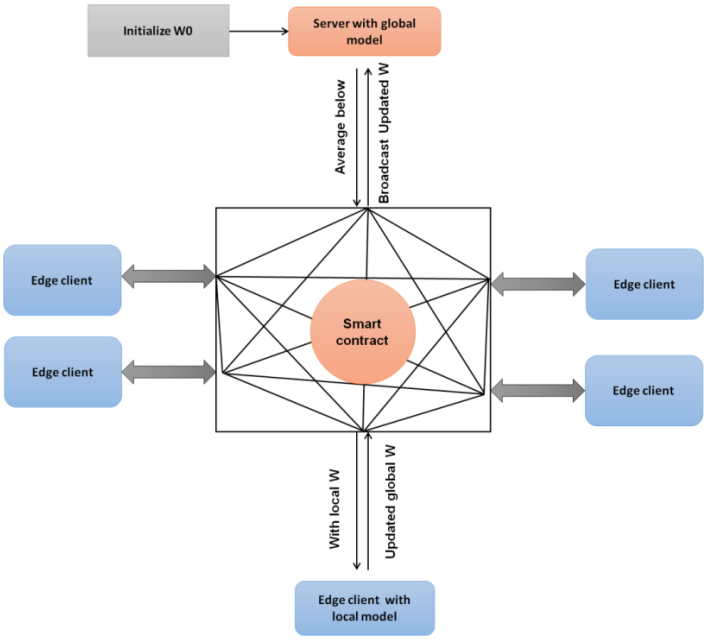

Figure 2. Representation of the FIDANN blockchain network

2.5. Description of the Detection model

The intrusion detection task is done by DMO-ANN. The DMO operates on the same concept as the randomized population-based metaheuristic algorithm. This method was designed to simulate the group dynamics and foraging techniques of the dwarf mongoose. Dwarf mongooses are social creatures that forage in groups, yet when it comes to eating, each animal acts independently. Because of their seminomadic nature, they construct a mound in which to sleep near a bountiful food supply and then move on to find the next similar source. As can be seen in Equation (1), the DMO begins its updates by establishing the initial values for the mongoose's candidate population. Populations are created randomly between the lower limit (LB) and upper bound (UB) of a given issue (UB).

$$N = \begin{bmatrix} n_{1,1} & n_{2,1} & \dots & n_{1,i-1} & n_{i,1} \\ n_{1,1} & n_{2,2} & \dots & n_{2,i-1} & n_{2,i} \\ \vdots & \vdots & n_{d,s} & \vdots & \vdots \\ n_{x,1} & n_{x,2} & \dots & n_{x,i-1} & n_{x,i} \end{bmatrix} \quad (1)$$

Where N is the collection of currently available candidates, produced randomly using Equation (2), $n_{d,s}$ is the coordinate of the ith population's jth dimension, x is the population's size, and i is the dimension of the problem.

$$n_{ds} = unifrnd\ (VarMin, VarMax, VarSize) \quad (2)$$

Where $unifrnd$ is a uniformly distributed random integer, $VarMin$ and $VarMax$ are the minimum and maximum allowable values, and $VarSize$ is the problem's size. As of this iteration, the best solution is the same as the finest solution in the prior iteration. The DMO, like other metaheuristic algorithms, consists of two phases: exploitation (in which individual mongooses conduct a comprehensive search in a specific location) and exploration (in which mongooses explore randomly for a novel abundant source of food or new Sleeping mounds (SM)). DMO's three primary social structures— the scout group, babysitters, and the alpha group, carry out the activities throughout the two stages.
The alpha female (α) in a family unit is chosen according to equation (3).

$$\alpha = \frac{fit_d}{\sum_{d=1}^{x} fit_d} \quad (3)$$

The x-bn symbol stands for the amount of mongooses in the group. Bn stands for the babysitters' number, and peep is the female alpha's sound, which keeps the family on the smooth path.

The position of the SM is determined by the plentiful food source, which is described in Equation 4 below.

$$N_{d+1} = N_d + phi * peep \quad (4)$$

where phi is a randomly distributed number between [-1,1]. The SM is assessed at the end of each cycle; Equation 5 is a representation of the sleeping mound.

$$jc_d = \frac{fit_{d+1} - fit_d}{\max\{|fit_{d+1} - fit_d|\}} \quad (5)$$

When an SM is discovered, Equation 6 provides a value that is representative of the average.

$$\varphi = \frac{\sum_{d=1}^{x} dc_d}{x} \quad (6)$$

As soon as the criteria for switching babysitters have been met, the process moves on to the scouting group (SG), when the next SM is evaluated based on the proximity to a suitable food source. Since mongoose often does not return to already-used sleeping mounds, the SG must always be on the lookout for new ones to guarantee exploration success. In DMOA, foraging and SG happen simultaneously on the assumption that the further the family forages, the higher the probability of identifying the next SM, as simulated by Equation 7.

$$N_{d+1} = \begin{cases} N_d - ME * phi * rand * \left[N_d - \vec{C}\right] & if\ \varphi_{d+1} > \varphi_d \\ N_d - ME * phi * rand * \left[N_d - \vec{C}\right] & else \end{cases} \quad (7)$$

The parameter ME $= \left(1 - \frac{\text{iter}}{\text{Max}_{\text{iter}}}\right)^{\left(2-\frac{\text{iter}}{\text{Max}_{\text{iter}}}\right)}$ that controls the group's volatile, collective motion of mongooses is linearly reduced with time, and the rand is a random value between [0,1]. The mongoose's desire to go to a new mound of dead leaves is represented by the vector $\vec{C} = \sum_{d=1}^{x} \frac{n_d \times jc_d}{N_d}$.

While the SG and foraging group seeks an SM and source, the babysitter's group stays with the youngsters. Since they don't forage or scout, this group's members are subtracted from the candidate population. As seen in Equation 7, the babysitters enter the foraging or scouting group to find food when a specific criterion is reached.

The ANN approach with backpropagation is utilized for the detection mechanism. Forward propagation in a neural network is used during the training phase. The output layer nodes produce a value after the forward pass. During the forward pass, the entire input to the node is first determined, and then the output of the node is determined using the activation function. This formula is used to compute the total input received by each neuron in a feed-forward neural network.

$$Total\ Input = f_1 * a_1 + f_2 * a_2 + \cdots + f_w * a_w + 1 * m_n \quad (8)$$

$$Where: f_1, f2, \ldots\ldots, ff\ -\ Input\ neurons$$

$a1, a2, \ldots\ldots, an$ – Weights associated with input neurons
a_n – Weight associated with bias Output of neuron is calculated using the activation function
To determine the neuron's output, the activation function is used.

$$Activationfunction = 1/\left(1 + x^{(-TotalInput)}\right) \quad (9)$$

Where:

Total Input – The total input to the neuron

Training artificial neural networks using a technique known as backpropagation, in combination with an optimization approach such as gradient descent, is widespread. Propagation and weight updates are the two phases of the algorithm's two-step cycle. Link weights are adjusted once the forward pass output is compared to the predicted output during the back-propagation phase. Figure 3 represents the architecture of ANN.

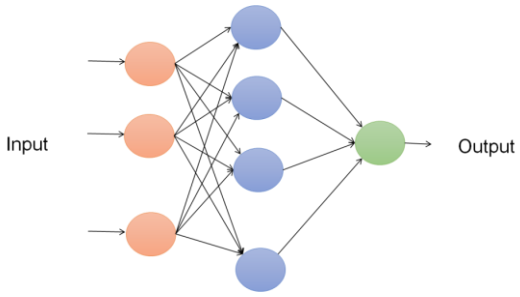

Figure 3. Representation of ANN

3. RESULTS AND DISCUSSION

In this study, we compare the efficiency of the proposed approach with that of the existing one. The parameters are security level, accuracy, precision, recall, and F1-score. The existing methods are CNN-TSODE, GIWRF, and IKNN. Regarding the classification of the IDS utilising TP, TN, FP, and FN (where true positive as TP, true negative as TN, false positive denoted as FP, and false negative as FN). The below table shows the formula for the parameters for the classification.

TP: it refers to the amount of connections that were identified as an intrusion in an appropriate way.
TN: An accurate negative classification prediction is referred to as a "true negative."
FP: The amount of intrusion connections that were misclassified as normal.
FN: This represents the number of regular connections that were misclassified as intrusions.

Table 1. Formula for the classification parameters

S.no	Parameter	Formula
1	Accuracy	$\frac{TP+TN}{TP+TN+FP+FN}$
2	Precision	$\frac{TP}{TP+FP}$
3	Recall	$\frac{TP}{TP+FN}$
4	F1-score	$\frac{2TP}{2TP+FP+FN}$

The accuracy rate is defined as the percentage of occurrences that were properly predicted relative to the total number of instances that were anticipated. Figure 4 depicts the result of accuracy in the standard and suggested methods.

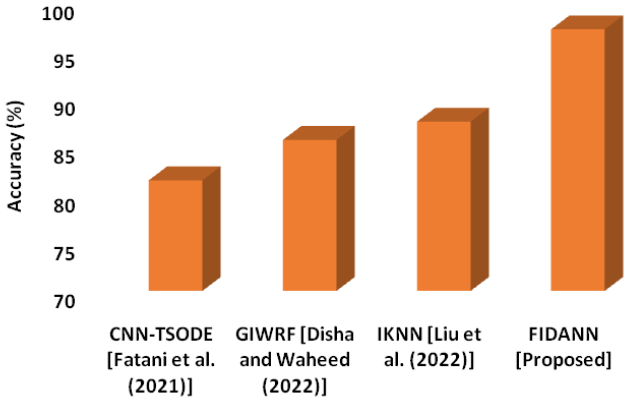

Figure 4. [20-22] Accuracy of suggested and standard methods

In comparison, the recommended techniques FIDANN obtains 97.2 % of accuracy value while CNN-TSODE obtains 81.5%, GIWRF obtains 85.7% and IKNN obtains 87.6 %. It reveals that the recommended technique is more effective in intrusion detection mechanisms than the one that is currently in use. The fraction of all assaults that are correctly identified is termed the precision rate. Figure 5 depicts the comparison of precision in the standard and suggested methods. In contrast, the suggested method (FIDANN) achieves 95.7% precision, compared to 80.12% for CNN-TSODE, 87.5% for GIWRF, and 83.8% for IKNN. It demonstrates that the suggested approach is better than the one currently in use in terms of intrusion detection mechanisms.

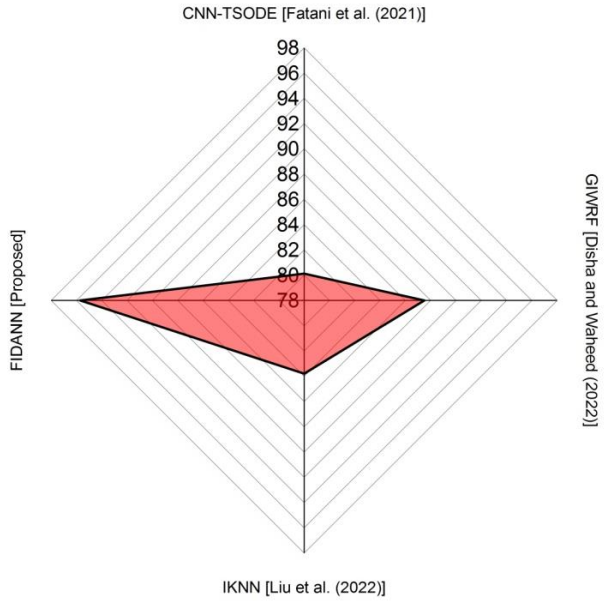

Figure 5. [20-22] Precision of suggested and standard methods

Recall rate refers that the ratio of assaults identified by the suggested approach to all actual attacks. Figure 6 depict the comparison of recall in the standard and suggested methods. The recommended approach (FIDANN) obtains 96.15% precision, but CNN-TSODE, GIWRF, and IKNN only achieve 89.33%, 85.13%, and 82.27%, respectively, of precision. It illustrates that the recommended method's intrusion detection technique is better than the one that is currently in use.

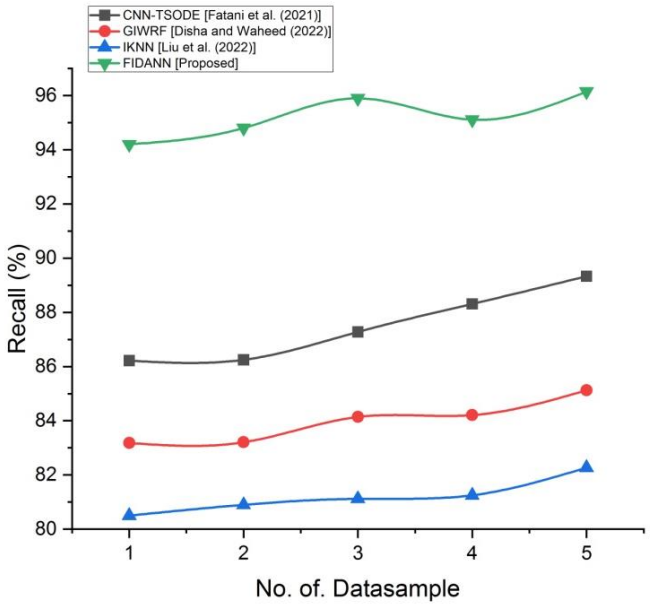

Figure 6. [20-22] Recall of suggested and standard methods

The weighted average of both accuracy and recall, which yields a single overall score for them, is the F1 score. Figure 7 depicts the comparison of the F1-score in the standard and suggested methods. When comparing current methods such as CNN-TSODE, GIWRF, and IKNN which have values of 89.32 %, 86.25 %, and 83.21 % with the suggested method (FIDANN) of 97.33 %. It concludes that the proposed method outperforms the current method of intrusion detection.

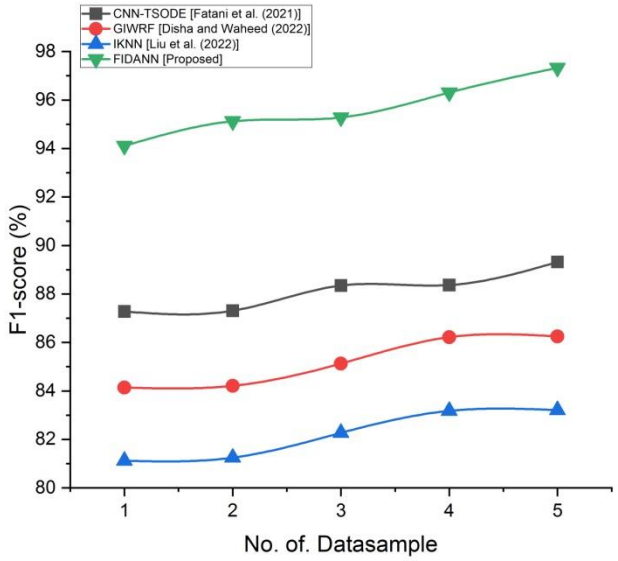

Figure 7. [20-22] F1-score of suggested and standard methods

4. CONCLUSION

In this paper, we present the FIDANN, an intelligent intrusion detection mechanism that protects the privacy of medical data by detecting intrusions using DMO-ANNs, or dwarf mongoose-optimized artificial neural networks. With regard to current advancements in blockchain technology, such as the removal of contaminating assaults and the convenient provision of complete visibility and data integrity over the decentralised system. By restricting the information that may be sent from the cloud's GW using the model at the edges, assaults can be prevented while using less computer power and time because FL only needs to

analyse a smaller amount of data. The experimental result such as accuracy (97.2 %), precision (95.7 %), recall (96.15 %) and f1-score (97.33 %) shows superior performance than the current methods. Future research should focus on enhancing the proposed FIDANN effectiveness by employing various categories to identify the sort of attack and identify its origin; this will help to safeguard healthcare systems even better.

REFERENCES

[1] Chatzinikolaou, T., Vogiatzi, E., Kousis, A. and Tjortjis, C., 2022. Smart Healthcare Support Using Data Mining and Machine Learning. In IoT and WSN based Smart Cities: A Machine Learning Perspective (pp. 27-48). Cham: Springer International Publishing.

[2] Salem, M., Elkaseer, A., El-Maddah, I.A., Youssef, K.Y., Scholz, S.G. and Mohamed, H.K., 2022. Non-Invasive Data Acquisition and IoT Solution for Human Vital Signs Monitoring: Applications, Limitations and Future Prospects. Sensors, 22(17), p.6625.

[3] Ashfaq, Z., Mumtaz, R., Rafay, A., Zaidi, S.M.H., Saleem, H., Mumtaz, S., Shahid, A., Poorter, E.D. and Moerman, I., 2022. Embedded AI-Based Digi-Healthcare. Applied Sciences, 12(1), p.519

[4] Dammak, B., Turki, M., Cheikhrouhou, S., Baklouti, M., Mars, R. and Dhahbi, A., 2022. Lorachaincare: An IoT architecture integrating blockchain and lora network for personal health care data monitoring. Sensors, 22(4), p.1497.

[5] Sahu, M.L., Atulkar, M., Ahirwal, M.K. and Ahamad, A., 2022. Vital sign monitoring system for healthcare through IoT based personal service application. Wireless Personal Communications, 122(1), pp.129-156.

[6] Chandan, Radha Raman, Awatef Balobaid, Naga Lakshmi Sowjanya Cherukupalli, Gururaj H L, Francesco Flammini, and Rajesh Natarajan. 2023. "Secure Modern Wireless Communication Network Based on Blockchain Technology" Electronics 12, no. 5: 1095. https://doi.org/10.3390/electronics12051095

[7] Kumar, N., Kaushal, R.K., Panda, S.N. and Bhardwaj, S., 2022. Impact of the Internet of Things and Clinical Decision Support System in Healthcare. In IoT and WSN based Smart Cities: A Machine Learning Perspective (pp. 15-26). Cham: Springer International Publishing.

[8] Li, G., Dong, M., Yang, L.T., Ota, K., Wu, J. and Li, J., 2020. Preserving edge knowledge sharing among IoT services: A blockchain-based approach. IEEE Transactions on Emerging Topics in Computational Intelligence, 4(5), pp.653-665

[9] Du, X., Chen, B., Ma, M. and Zhang, Y., 2021. Research on the application of blockchain in smart healthcare: constructing a hierarchical framework. Journal of Healthcare Engineering, 2021.

[10] Arvindhan, M., Thirunavukarasan, M. and Daniel, A., 2022. Blockchain Technology in the Energy Sector: A Systematic Review of Challenges and Opportunities. Handbook of Green Computing and Blockchain Technologies, pp.107-118

[11] Xu, J., Glicksberg, B.S., Su, C., Walker, P., Bian, J. and Wang, F., 2021. Federated learning for healthcare informatics. Journal of Healthcare Informatics Research, 5, pp.1-19

[12] Kumar, P., Kumar, R., Gupta, G.P., Tripathi, R., Jolfaei, A. and Islam, A.N., 2023. A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system. Journal of Parallel and Distributed Computing, 172, pp.69-83

[13] Natarajan, Rajesh, Gururaj Harinahallo Lokesh, Francesco Flammini, Anitha Premkumar, Vinoth Kumar Venkatesan, and Shashi Kant Gupta. 2023. "A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0" Infrastructures 8, no. 2: 22. https://doi.org/10.3390/infrastructures8020022

[14] Muhammad, G., Hossain, M.S. and Garg, S., 2020. Stacked autoencoder-based intrusion detection system to combat financial fraudulent. IEEE Internet of Things Journal

[15] Keshk, M., Turnbull, B., Moustafa, N., Vatsalan, D. and Choo, K.K.R., 2019. A privacy-preserving-framework-based blockchain and deep learning for protecting smart power networks. IEEE Transactions on Industrial Informatics, 16(8), pp.5110-5118.

[16] Weng, J., Weng, J., Zhang, J., Li, M., Zhang, Y. and Luo, W., 2019. Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive. IEEE Transactions on Dependable and Secure Computing, 18(5), pp.2438-2455.

[17] Singh, M., Aujla, G.S., Singh, A., Kumar, N. and Garg, S., 2020. Deep-learning-based blockchain framework for secure software-defined industrial networks. IEEE Transactions on Industrial Informatics, 17(1), pp.606-616.

[18] Gadekallu, T.R., Manoj, M.K., Kumar, N., Hakak, S. and Bhattacharya, S., 2021. Blockchain-based attack detection on machine learning algorithms for IoT-based e-health applications. IEEE Internet of Things Magazine, 4(3), pp.30-33

[19] Akshay Kumaar, M., Samiayya, D., Vincent, P.M., Srinivasan, K., Chang, C.Y. and Ganesh, H., 2022. A Hybrid Framework for Intrusion Detection in Healthcare Systems Using Deep Learning. Frontiers in Public Health, 9, p.2295.

[20] Fatani, A., Abd Elaziz, M., Dahou, A., Al-Qaness, M.A. and Lu, S., 2021. IoT intrusion detection system using deep learning and enhanced transient search optimization. IEEE Access, 9, pp.123448-123464.

[21] Disha, R.A. and Waheed, S., 2022. Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest (GIWRF) feature selection technique. Cybersecurity, 5(1), p.1.

[22] Liu, G., Zhao, H., Fan, F., Liu, G., Xu, Q. and Nazir, S., 2022. An enhanced intrusion detection model based on improved kNN in WSNs. Sensors, 22(4), p.1407.

BIOGRAPHIES OF AUTHORS

Priyanka Tyagi is working as an Assistant Professor at the Department of Computer Science & Engineering, Sharda University. She has completed her B.E in CSE from MDU, M.Tech in CSE from Banasthali Vidyapeeth & completed Ph.D from Linagayas Vidyapeeth. Her topic of research was "Design a Hybrid Classification Approach of Sentiment Analysis of Twitter Data". Dr. Priyanka Tyagi has 10+ years of Teaching Experience in various technical Universities/ Institutions. She is Mentor of NPTEL course and guiding research investigations for under-graduate, post-graduate engineering students in the areas including Machine Learning, Software Engineering, Artificial Intelligence, Database Management System. She can be contacted at email: priyanka.tyagi@sharda.ac.in.

S.K. Manju bargavi completed her M.E (CSE) at Anna University, along with a PhD degree in Wireless Ad-hoc Network at Anna University, Chennai, Tamilnadu. She has 19+ years of experience in which 1.3 years of industry experience and 5 years of Abroad experience. She has published papers in reputed National and International journals, conferences, Patents (9) and books (4). She has applied research fund in Government organization. She has got "Best Innovation Teacher award" from Aurobindo society for national level. She is strong willed, self-motivated, result oriented and enthusiastic to learn & adapt to new technologies. Her areas of intense research and scholastic teaching are Wireless Ad-hoc Network, IoT, Network Security, Image processing, Computer Graphics, Operating system using Linux, Computer Architecture, C, C++, Java and Python. She can be contacted at email: b.manju@jainuniversity.ac.in.