Computer Systems Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2023.038085

ARTICLE

Intrusion Detection and Prevention Model for Blockchain Based IoMT Applications

Jameel Almalki*

Department of Computer Science, College of Computer in Al-Lith, Umm Al-Qura University, Makkah, Saudi Arabia

*Corresponding Author: Jameel Almalki. Email: jamalki@uqu.edu.sa

Received: 26 November 2022 Accepted: 17 February 2023 Published: 26 January 2024

ABSTRACT

The recent global pandemic has resulted in growth in the medical and healthcare sectors. Applications used in these domains have become more advanced and digitally integrated. Sensor-based Internet of Things (IoT) devices are increasing in healthcare and medical units. The emerging trend with the use of IoT devices in medical healthcare is termed as Internet of Medical Things (IoMT). The instruments used in these healthcare units comprise various sensors that can record patient body observations. These recorded observations are streamed across Internet-based channels to be stored and analyzed in centralized servers. Patient diagnostics are performed based on the information retrieved from these devices. Machine learning and artificial intelligence play a significant role in diagnostic mechanisms and identifying diseases across observation sets. The data collected by these observation sets are analyzed closely with the help of Artificial Neural Networks (ANN). This distributed system of devices and servers raises privacy concerns. Blockchain is a technology that can preserve the privacy of the information collected from devices. A blockchain is a mechanism in which information goes across various network nodes. A centralized architecture where information flows from the sensor devices to a centralized server risks large-scale information leak. This paper proposes a prototype and a model for collecting information and protecting the data from intrusion. Any application that resides in the cloud and collects data from a sensor based IoT device can be prone to intrusion. The detection occurs at an early stage and in a fraction of the time. The model uses artificial neural networks and gets evaluated across various datasets. Improved accuracy and performance with data analyzed at the IoT-based devices prove the efficiency of the model proposed in this study. The stability and accuracy of the results after testing these applications make the model sustainable and acceptable across healthcare systems.

KEYWORDS

Intrusion; blockchain; IoMT; applications; machine learning

1 Introduction

In the recent past, the Internet of Things (IoT) has gained importance in various sectors of day-to-day living. Medical and healthcare facilities are one of the most critical industries of humanity. IoT has entered this domain and provides various brilliant improvements. Medical data sourced from sensor enabled IoT devices is a crucial step for medical practice [1]. In the past, there was a requirement for a nurse to be available always to record various readings of a patient's biological factors. Devices

minutely observed the biometric characteristics such as heart rate, temperature, pulse rate, blood pressure, and oxygen level with the help of human intervention [2]. More recently, devices can monitor these vital signs, and they can make observations with the use of sensor-based devices. Study [3] suggested a system comprised of continuously monitored wearable devices to identify the healthcare parameters of a patient. Model streamed the information collected by these wearable devices for analysis at a remote site. This information was sent from the devices and made available for a doctor's timely analysis of critical conditions. The study comprised a combination of devices limited to a specific biometric factor recognition. Another study [4] suggested architecture to minimize the number of visits by a doctor to a site near the patient. The health parameters considered were controlled with this system's help, and the plan is simple and efficient. Observations calculated that the system saved approximately 56.9% of energy consumption as per the observations. The system's contribution was using sensor-based mechanisms and green computing supported by IoT communications. It enhanced the throughput, and the outcome of the system was excellent. The performance of the system parameters considered by the doctors helped diagnose and treat a patient. The big data collected with the help of Information Systems replicates across various cloud servers. These cloud servers accept data from multiple sensor-based devices in the form of specialized data packets.

The system proposed in this study contains the following entities:

- An intrusion detection model that can help to protect an IoT-based healthcare system. The suggested model expects to be a lightweight process that will take care of the minimal resources available at the IoT device and all the edge nodes. The memory constraints and the computational power of the small IoT devices are major factors for selecting and proposing a lightweight model. The dataset that the model will create with the help of observations accumulated by these IoT devices will work with an artificial neural network. It is well-known that the information retrieved from IoT-based devices is of colossal quantity when connected to an IoT-driven healthcare unit. Therefore, the artificial neural network can handle large datasets easily and provides better performance.
- There are various problems associated with data failure during transmission and reception, including privacy issues and training of the model data from the data in any healthcare application. The proposed model comprises a cloud computing architecture integrated with an intrusion detection system with the help of edge computing devices. The detection response toward the information flow and intrusion will be faster in edge nodes than in traditional network nodes. That is why the overall workload of the environment will be low. Thus, the computation power will be on the higher side.
- The main ingredient of the proposed model is the amalgamation of Blockchain with the above-stated sections of the model. Blockchain can maintain any poisoning attack, whether on a model or related to data, and the concerned user's privacy with the system's help. Moreover, a blockchain environment can achieve the transparency of the information along with the distributed data modeling and training procedure successfully in a blockchain environment.

The introduction to the technology is described with reference to recent research in Section 2. The paper continues with Section 3 on Materials and Method, providing a complete description of the architecture proposed for this model. The methodology followed for the detection of intrusion is also presented. Section 4, Results, provides the preprocessed and trained datasets to be used in the model proposed in this study. A complete discussion and comparison with other proposed models are made in this section. The section also covers results from various datasets collected across open-source

repositories. Finally, Section 5, Conclusion, provides a detailed description of the proposed model and the prospects related to the study.

2 Literature Review

Any distributed system that integrates devices requires the definition of a packet format for the data that travels from the sensor to the cloud server. The central server in this kind of architecture is a single-point failure, which is one of the most significant drawbacks of these systems. Having the information and resources in a single place is a problem regarding data sharing and analysis [5]. As per a study by [6], the availability of information in a centralized repository or a centralized server-based location is more prone to data and privacy leakage. Study [7] proposed a solution for this problem that uses blockchain technology to store information across centralized servers. The network nodes communicating in the Blockchain will hold the information decentralized across various nodes in a Peer-to-Peer (P2P) network. The transmission of information and transaction processing in the blockchain network allows simultaneous storage and broadcasting of the information across all the nodes. Cloud environments can use the consensus algorithm and smart contracts within the Blockchain to ensure data privacy and security of critical data stored in the cloud environment. Study [8] claimed that data resides in distributed nodes across the distributed ledger in the Blockchain, which solves the privacy leakage problem arising from a centralized repository or server. Amongst various vital factors provided by the blockchain network, security, privacy, and the decentralization of the information are the most beneficial ones. It is critical in healthcare settings, with observations from various sensor-based devices recording copious amounts of data.

The information received in cloud storage comprises many data bits and bytes. Storage done in the Blockchain is safeguarded with the help of various encryption keys to ensure the safety of user identity. Study [9] supported privacy preservation for multiple patients' medical records across a blockchain network. The tampering of the information gets minimized in this case. The analysis of the system that the author proposed ensured that the system had well-preserved security in association with the fewest errors, a low ratio for data loss, less time for the generation of data packets, and maintenance of transparency of the information [10]. Preparing a block in any blockchain network takes the minimum possible data handling and processing time. Many factors support the use of IoT devices in association with blockchain technology to ensure data preservation, robustness, transparency of information, avoidance of data breaches, and the provenance of data [11]. Various applications in the healthcare industry run with a blockchain-based network for security preservation and data transparency. Study [12] suggested a system comprised of management of the data collected over the Blockchain. The model represents the identification of data records and information management across them. Study [13] reported a system for the management of information and patient vital biometric data. The information collected over a remote monitoring blockchain comprises patient information with the help of the system. Study [14] made use of a blockchain network to manage and manage the feasibility of drug counterfeiting. These systems can work with medicinal drugs with the help of this blockchain-based system. Study [15] proposed a fantastic system that provided contact tracing of patients and contained the spread of diseases. The author designed the plan for any infection that flourishes in a global pandemic like COVID-19.

Usually, healthcare services make use of IoT devices to collect information and send it to a centralized cloud server. However, the services offered by these IoT devices can also be under threat. The information that flows from these devices can be hacked, resulting in unethical use. IoT botnets

are usually responsible for such issues, which raise the problem of remote access to these devices [16,17]. The information that is available across these devices is very vulnerable to attack as well as leakage. In addition, problems exist associated with the infringement of the information that flows across these IoT-enabled systems [18]. Distributed denial of services and ransomware are also a class of threats to IoT-based devices and the services offered [19]. Botnet attacks are one of the most crucial research areas aimed at maintaining privacy and security, including authentication issues for healthcare systems. The use of machine learning-based applications is one of the critical factors that can reduce the chances and problems associated with this case. Machine learning-based models provide a two-way solution for data diagnosis along with the conceptualization of maintaining the secrecy and privacy of the system [20].

Intrusion detection and prevention of security breaches and problems like botnet attacks or Uniform Resource Locator (URL) phishing can be controlled and handled with the help of tools like data mining and machine learning-based models [21]. Due to the constantly available resources in the IoT domain of applications, it is necessary to provide intrusion detection and prevention system for IoT devices [22]. A fascinating method was proposed by [23] that comprises a barcode scanner used to authenticate a user responsible for accessing information from a cloud server connected to an IoT-based application. The system did a secure analysis of the information for a patient based on the barcode. The doctor and the healthcare unit manage this data with probable diagnosis and feedback. A machine learning model was used to train the data and the information in the cloud. Finally, the system processed the data restored to the cloud server to provide a proper diagnosis of the patient's disease. Yet another unique method was proposed by [24], which used a convolutional neural network for intrusion detection. Pattern recognition was the main feature of this system in which classification was done based on traffic attacks. Models identify the attack pattern, and the model gets trained so that the system can oversee such attacks and restrict unethical access to the information. Prediction of attacks in a network based on factors like malicious operations, unauthorized access, traffic analysis, and data probing was given by [25]. The author did a comparative study with the proposed model compared to support vector machines, decision trees, and artificial neural network models. Compared with all the existing models, the efficiency for detecting attacks with the proposed model's help was 5.6% more than previously existing solutions.

The problem of latency and loss of data due to network paths and crowding are significant problems for cloud computing applications and access [26]. Due to latency issues when communicating via cloud computing environments, edge computing paradigms have been suggested to support IoT applications [27,28]. The core ideology behind edge computing is to hold the data obtained from these IoT devices at the edge of the network rather than in the core network. Cloud computing-based applications communicate the data from the IoT device and then access the information over the traditional web. The data is processed at the edge device and submitted to the cloud server [29]. It improves data access performance and enhances the processing capability's quality across a cloud computing environment [30]. This combination of edge network and the cloud computing application is assumed to perform better than traditional architecture.

Researchers deployed various intrusion detection and prevention systems proposed by several researchers in a cloud environment. Still, they could not support the security requirement for real-time data monitoring from different healthcare devices. The potential loss of information occurs in an environment where intrusion detection occurs but with a time delay. The vulnerability of a data breach and IoT device tampering is likely in cases where there is a delay in detecting unauthorized or unethical access [31]. The training of a data model happens after the classified data gets uploaded to the cloud environment. But the transfer of this information may affect the integrity of the data. In such

cases, intrusion detection can be time-consuming based on multimedia data collection. Guaranteed verification of text or videos is costly in terms of time [32]. The model can compromise the security of the healthcare unit because of such issues. Therefore, intrusion detection and prevention are necessary for the hour. Various real-world problems were solved with the help of techniques like deep learning as well as machine learning.

The contributions of these technologies are remarkable; however, they have several issues. Study [33] suggested an impressive way for data collected by a smart device to be trained and overseen by itself. Centralized learning will regulate the data, or edge devices will process the information at the edge layer on the edge device. Finally, once the information is processed, it will transfer to the server in the form of updates. The model's training will be a continuous repository-based process that will execute across all the edge devices connecting to this application. All the updates and collection of trained model data will get broadcast to all the devices across the network. It ensures the privacy of the data processed at an edge level and reduces the chances of a data breach. Study [34] suggested yet another deep neural network model for evaluating the data sets and proposed an algorithm responsible for having a remarkably high detection rate. The algorithm presented here reduces the overhead needed for identifying unauthorized access. The use of logistic regression and the artificial neural network to preserve data integrity and privacy of an individual's healthcare information was proposed by [35]. However, the model proposed by the author needed to be improved compared to an artificial neural network. Digitization of medical data is one of the most crucial factors required for the global availability of data sets. However, Study [36] suggested that the centralized repository and concentration of the datasets are optional. The author said that sensitive information could have various issues in centralized server-based systems. The author also suggested that multiple attacks, like data poisoning, can lead to enormous challenges. There are chances that private data can be compromised [37]. Data poisoning is when an attacker introduces malicious data to an existing data packet. This additional data will hinder and change the training data set, resulting in unexpected results. A similar representation was presented by [38], which proved the poisoning parameters for the training dataset. Study [39] suggested that the poisoning of a dataset can be managed and managed with various techniques; however, the poisoning of the data model is indeed more dangerous in comparison. A probable solution was proposed by [40] in which data poisoning takes place. The private data gets replicated as a clone in the cloud. After the leading training of the dataset was completed yielding a poisoned model, the clone from the cloud application replaced the dataset. The global model remains unaffected despite the model poisoning. It is also worth mentioning that the data also remains private and safe.

There have been various models and proposed architectures that can avoid the problem of poisoning attacks. Poisoning can reduce the model's performance by providing multiple updates towards poisoning in the algorithm. The main task for the model can be hindered and may face consequences, as per the author. The amalgamation of various new technologies like encryption and Blockchain can provide a better solution to the problem associated with the models. Study [41] recommended an imposing model that used blockchain technology and a deep learning framework. The proposed solution oversees various cyber-attacks expected in a cloud environment application. The framework that the author proposed yielded better performance against poisoning attacks. As per the expectation, the system also safeguarded the privacy of the information in the proposed model. The transaction of the information preserves the security of the data. It also manages the integrity of the information with the help of Blockchain. The model aggregation and the protection of IoT security across various systems will be helpful in healthcare units.

3 Materials and Methods

3.1 Proposed Concept

Various models have been proposed concerning this topic. One model [42] comprised various layers responsible for different tasks. Yet another exciting model [43] comprised a system responsible for detecting an intrusion at edge nodes. Finally, the edge computing layer manages the entire system's security and privacy. Fig. 1 below represents the intrusion detection logic at the edge layers. The layered architecture and a comparison of the proposed model with previously benchmarked models are presented in the subsequent figures. The layers taken into consideration are the business, edge, and IoT connectivity layers (healthcare layer). The system proposed in this study comprises of machine learning-oriented model which exchanges the vital information of a patient's biometric data with the help of smart contracts in the Blockchain.

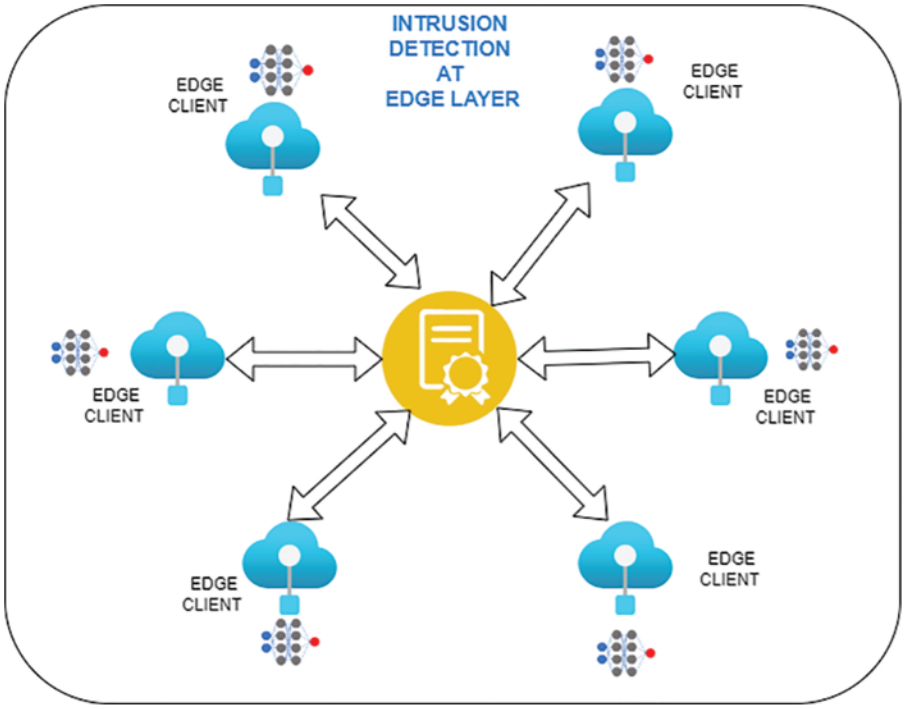

Figure 1: Edge layer detection for ANN-based intrusion detection

The data is first analyzed for diagnosis with the help of a machine learning (ML) algorithm. The system proposed by [13,43] needs to address security parameters and the issues for intrusion detection or prevention. The centralized server-based application makes it difficult and more prone to poisoning attacks. The models above do not discuss single points of failure and the risks of compromising critical medical information when sending data to the centralized server. There needs to be a precise specification about various layers, and the system's security across these layers in the architecture proposed [43]. However, using edge layer devices resolves the problems inherent in the centralized server-based approach by removing the single-point failure and the risk of poisoning attacks. The architecture for the proposed study is shown in Fig. 2 below:

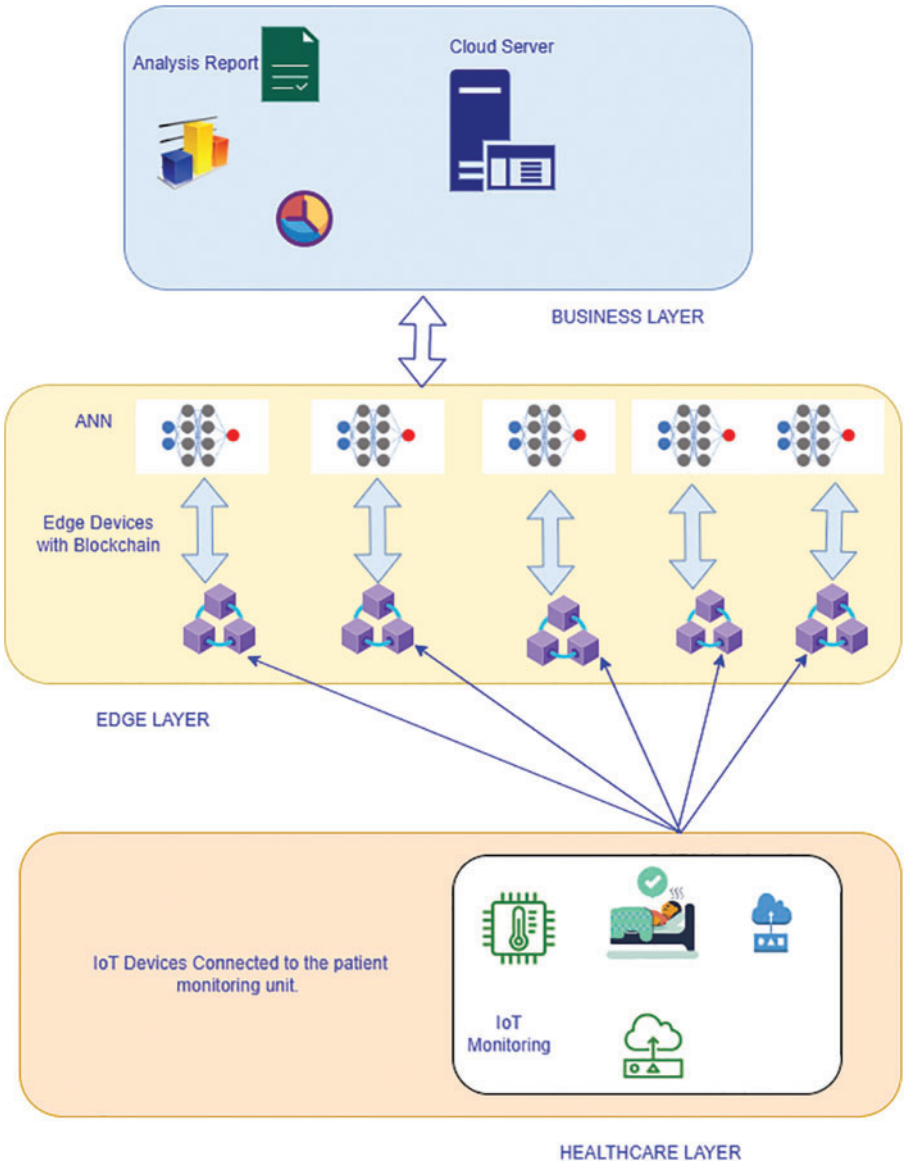

Figure 2: Proposed architecture for the intrusion detection system with ANN edge device

The architecture proposed in this study addresses the anomalies of previous models proposed by other researchers. The most frequent problem identified was the risk of a poisoning attack and the problems associated with single-point failure. The cloud application resides as a centralized system responsible for analyzing and diagnosing the information uploaded. The application is responsible for sending updated copies of weights to all the edge nodes. Once the nodes get updated, the cloud will do the data analysis at every edge level with the help of the new rules pushed by the cloud application. The final data created will be appended to the Blockchain with the help of smart contracts. The layered architecture proposed under this model is described below:

- Healthcare layer: the initial and foremost layer comprises all the IoT devices connected to provide the data from various healthcare units. The patient's health monitoring is done with the help of these devices that continuously stream information across the edge nodes. In addition, the edge-connected nodes safeguard against the problems of the centralized server network architectures used across other applications.
- Edge layers: the IoT-enabled devices are connected to the edge gateways. All the gateways comprise certain sensing devices capable of monitoring the biometric information of a patient. These devices do not connect with the global protocol, instead using their communication methods. The gateway is responsible for managing the data released from individual IoT devices. The observations collected by these edge devices are sent to the edge server, where they are analyzed for intrusion. The normalization of the data is done with the help of artificial neural networks at these points. The training of the model is done initially at the edge devices. Thus, it becomes simpler to identify whether any attack happens across the data packets. The tracking is done at the edge layer as soon as the data block is released from the gateway. Since the data at the initial level is protected, the detection time for any intrusion attack gets reduced. Thus, in this case, the resources will be safe, and the system will not compromise privacy for any data going from edge devices to the cloud. Another requirement is to work with the resources available at the edge for managing the information. IoT and server or computing devices are not required to check and address the issues at the macro level. Once the module gets trained, the ledger will add the final data collection resulting from the intrusion check to a distributed ledger in the Blockchain. The cryptographic functions which connect the Blockchain are responsible for managing any changes or manipulations done with the data. This mechanism shields the data from undetected poisoning attacks, which, if they occur, will be tracked immediately. The overall system architecture is described above in Fig. 2. Once the data gets collected from all the devices connected at the edge layer, the complete dataset gets encrypted with the help of cryptographic techniques and hash functions. The intelligent contracts verify that the data packets from valid sources reach valid destinations. Upon receipt of any data packet at the destination, a reverse procedure is performed to retrieve the original data. The prototype model constructed in this study deploys a hyper ledger fabric blockchain at a local network for testing purposes. This hypothetical Blockchain reflects the identification of the smart contracts exchanged between two parties regulated with an encrypted cryptographic identity.
- Business intelligence layer: this layer is responsible for managing information and analyzing the data by providing proper reports and mechanisms to keep a check on the data. With the help of smart contracts, the exchange of information is also managed by this layer, where transaction management takes place. All the business logic for updating the weights in the Blockchain takes place in this layer. This layer is one of the most important parts of the proposed model due to the availability of machine-learning algorithms. The model will use the data analyzed in this layer for patient diagnosis and disease identification. This layer is also responsible for identifying if there is any flaw between the various peer nodes.

The proposed algorithm below represents the working schema for the incoming data packets and the logic for checking intrusion. The rules specified in the ML schema will update the edge nodes based on their detection results. All the nodes in the Blockchain will undergo this procedure, and once there is no detection of intrusion, the ML rules are updated, and smart contracts are exchanged between the edge server and blockchain nodes.

Algorithm:

Input: nN is the number of nodes at the; Gr is the global value of the round off; c is the local values of the epoch; Bs = batch size; Eg = edge gateway number; nEg = size of data partition at the node of the edge gateway device; and Lr is the rate at which the system understands.
Output: the improved value of the weight at the machine learning algorithm for intrusion management

```
edgeServer ():                                  //Procedure
weight = 0
nN = First blockchain node                      //Node initialization
nN -> Connect to Blockchain
for (all EdgeNode: in c) do
        nN = nN + 1
        nN = c + 1                                      //Accessing all nodes
        nN = access all nodes for Hash check in the Blockchain
        nN = connect to destination IP
 end for loop
 nN: sends first weight
 for (all Gr : in nN), do
        for (all nN : Blockchain), do
                edgeServer (nN)
                Wf = Wi + W0
        end for Loop
 W_f = Sum (all Wi)
 end for loop
 end Procedure edgeServer ()
 edgeServer (nN, Wf)
 Bs <- Split Node data for nN                   //nth node data split
 for (all nodes : c), do
        Wc = W–Lr * F(Wi)                               //update local weights in backpropagation
 end for loop
 nN Publish local weight to the Blockchain
 nN -> Smart_contract_exchange ()
 update blockchain with nN across all P2P nodes
```

Fig. 3 presents the various activities in the proposed architecture. At the initial layer, the medical IoT units send information or biometric data of a patient to the edge gateway devices. These devices have restricted computational resources but can store a predefined dataset. Data training takes place at the edge level, and intrusion detection is performed simultaneously with the help of the machine learning model, which is trained to identify any intrusion. The detection rules get modified with the help of weights available inside the perceptron result. The rules must be reflected and updated across the network whenever a new intrusion is detected. Once the rules are updated, and intrusion is not found, the data that the edge devices have collected are collectively sent to the hyper ledger for the Blockchain. At the blockchain level, the smart contracts exchange takes place between the edge devices and the chain nodes. Once the devices are identified to be authentic and the exchange hash function results in proper authentication, the final authorization takes place. After the final approval, the information is updated in the blockchain nodes. Across the P2P network, data is broadcasted to the decentralized nodes. Once the nodes are updated, the data is finally sent to the cloud-based server.

The application takes control of the data and is finally saved inside the main centralized database. The data saved in this location is now available for analysis and reporting via the business logic. At this level, the data of the patient is visible to the healthcare units, including the hospital and doctor, along with the patient. Once the data is updated and analyzed correctly by the doctors, a proper diagnosis of the patient's sickness can be made easily. The blockchain nodes contain globally shared information.

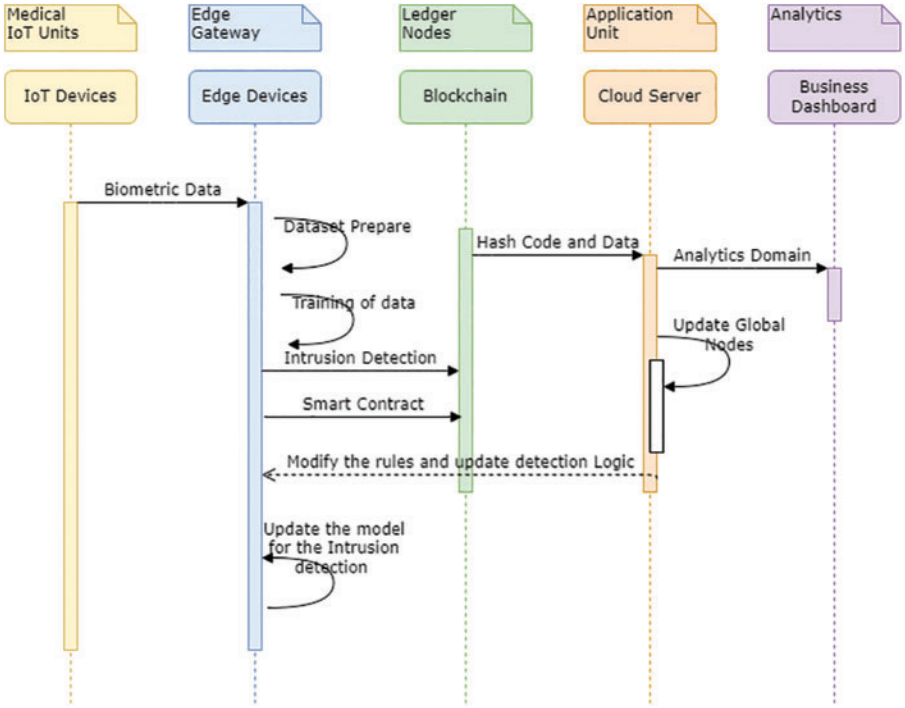

Figure 3: Activity diagram for the proposed model using blockchain for IoMT devices

In situations like pandemics, when information is required as the highest priority, these blockchain nodes can function as the fastest means of transport of information across the globe. In this way, the information moves on to the next level and can be used for dashboard entries across various applications. Once the memory update is committed, the IoT-based healthcare units' data flow back to the edge-level devices. At the network layer, these devices check for intrusion based on the machine learning rules that are updated inside the memory of the edge device. Once these devices receive information about intrusion detection, the data is immediately blocked and is not replicated across the blockchain nodes. Successful intrusion could result in errors like poisoning attacks. The detection mechanism ensures that the network will stop any changes in the data blocks at any level. The detection rules are based on the machine learning algorithm that runs with the help of an artificial neural network-based training model. The perceptron training assures that the data packet has the correct information. Any symptom of intrusion that takes place against the rules is immediately tracked. Data packets without issues are forwarded to the next level in the blockchain. Secrecy in the blockchain network is maintained with the help of smart contracts. The two parties contributing to the sharing and exchanging of information are called peers in the blockchain network. The peers belong to a particular channel in which the transmission of information takes place. The channel is responsible for overseeing the entries and transactions in the hyper ledger for the Blockchain. Inside the channel, the secure cryptographic key exchange takes place between the two entities responsible for exchanging

the smart contract. The smart contract is a piece of software that authenticates the cryptographic keys of both parties and acts as a mediator between the exchange. Once the smart keys are found authentic, the authorization of the two parties takes place in the Blockchain. Since it is assumed to be very safe and secure, the blockchain entities can now exchange data across the decentralized P2P network. Various frameworks are available across the world for deploying the Blockchain. However, for transaction-oriented blockchain models, the hyper ledger is one of the more successful frameworks. The experimental setup for this prototype model comprises a similar type of hyper ledger for deploying the Blockchain. The intrusion detection at the edge level takes place, and the final information, which is clear and authentic, is shared across the P2P network with the help of the blockchain smart contract authorization.

3.2 Intrusion Detection in the Model

The proposed architecture in this study makes use of the artificial neural network, which is a derivative of functions associated with the biological brain of a human being [44]. The multilayer perceptron is an efficient and commonly used elements of an artificial neural network [45]. The training of the model in this study comprises the steps used in the backpropagation algorithm for a feedforward network. The training is done based on the weight values calculated in Fig. 4 below. The dataset trained with this model's help is called the Bot-IoT dataset. The stochastic gradient descent (SGD) algorithm is used to optimize the values in this model. The sigmoidal activation function is used to activate the perceptrons in the multilayer neural network. Binary classification is used with a batch size of 100–1000. The number of local nodes that were trained in this model has the local epoch value 2–10. While evaluating the model for the proposed architecture in this study, certain assumptions were made. These assumptions are:

- All the parameters used for training will remain constant for various partitions in the actual dataset under consideration.
- The initial weight for all the nodes will remain the same without any variations in the values.
- Synchronous update of the values of the weights is done to all the respective nodes irrespective of the occurrence of the node during the analysis.
- The learning rate for all the nodes is equal in all the cases.

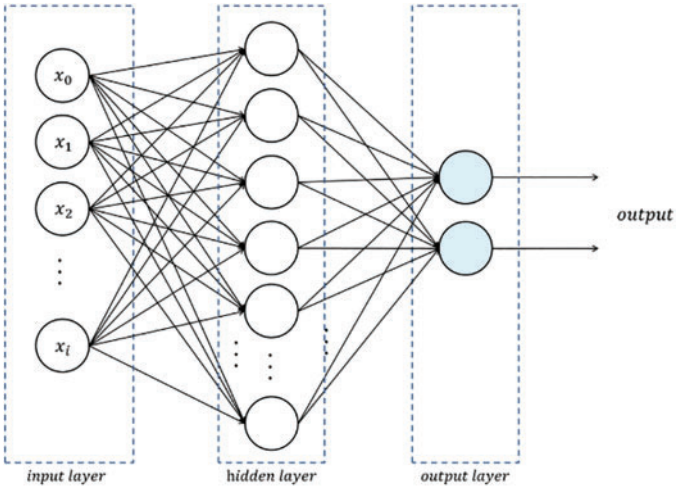

Figure 4: Artificial neural network intrusion detection model to achieve binary classification

The model proposed works on the Artificial Neural Network model for classification and intrusion detection. As shown in Fig. 4 above, the inputs from various edge devices reach the edge server. The rules for intrusion detection are available in the hidden layer. Once the data training is done, testing of the data takes place in this hidden layer. The rules are updated just in case any intrusion is detected. Once the information is found eligible to be committed to the Blockchain, it moves ahead, and output goes to the blockchain node in the P2P network.

4 Results and Discussion

The proposed model is evaluated with the help of an artificial neural network using an open-source dataset called BoT-IoT. This dataset was created in a genuine environment in a cyber-security lab at the University of New South Wales (UNSW). The dataset was set up with the help of information related to botnet attacks on IoT devices. More than 70 million records comprising various attributes were collected in this dataset [46]. For the model in this study, only 5% of the total dataset values were considered at the beginning [19]. Therefore, the results were compared with various datasets after the initial evaluation was completed. The results for all the comparisons are shown below. System and software characteristics used in the experiment were:

- The working environment comprised a high-end machine containing a Xeon processor with 32 GB RAM and an Nvidia GPU card.
- The analysis was done with the help of the Python programming language. Keras and PyTorch libraries were used for machine learning. Tensor Flow was used for the engine responsible for managing the data at the backend.
- This study used an Apple iMac with 16 GB RAM and an M1 Chip to deploy a blockchain and exchange the smart contracts. The deployment of the hyper ledger for the local network is done in this study, with the help of this machine, to demonstrate the prototype of the secure exchange of data in the model.

Fig. 5 shows the experimental setup of the blockchain ledger deployment at the local test network. The local test network contains two peers exchanging information after the smart contracts are exchanged. The blockchain hyper ledger is deployed on a centralized server. The two entities sharing smart contracts for data exchange are called peers. The two peers belong to the same organization. The channel is responsible for data transfer and smart contract exchange. Once the smart contracts are exchanged then, the blockchain data is appended to the nodes. The Fig. 5 represents that the approval take place once the smart contracts are exchanged. Then the information is sent from one peer node to another.

Fig. 6 presents the deployment of a blockchain test network to demonstrate the intelligent contract exchange in the proposed model prototype. The ledger on the Blockchain is mounted in the test network using the docker image. The peer entities are loaded and can be accessed for smart contract exchange. The test network assures the security of channel transfer and the secure exchange of smart contracts.

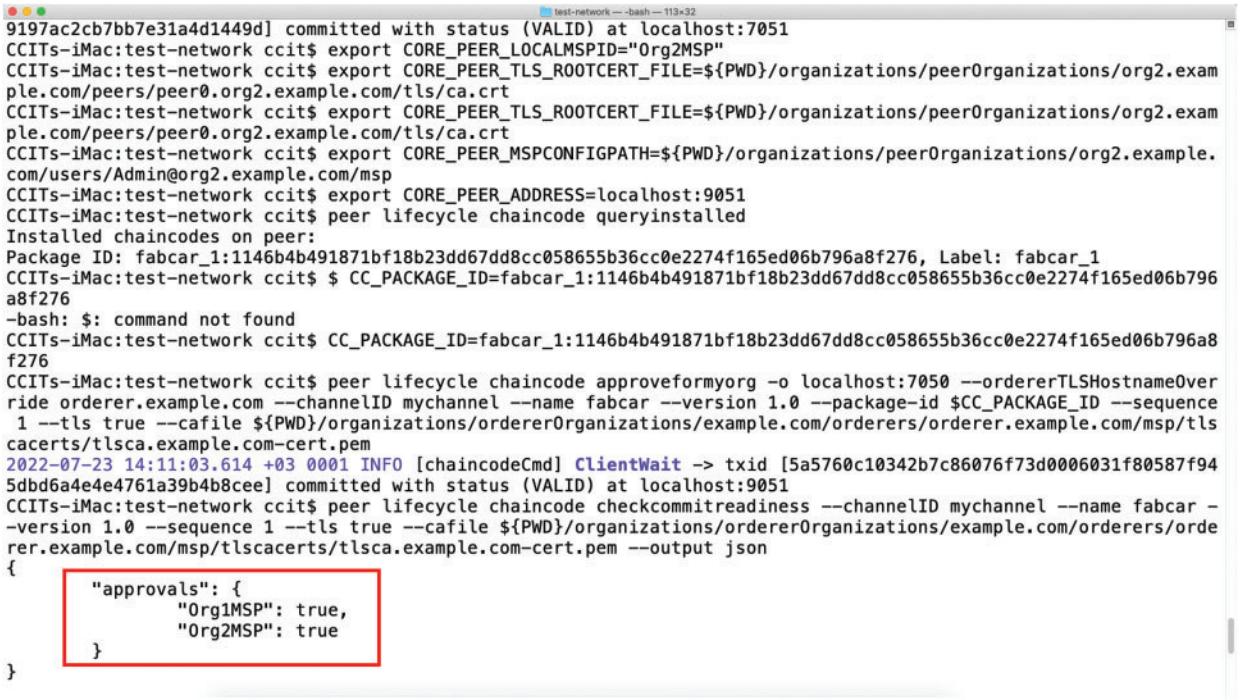

Figure 5: Blockchain smart contract exchange across a test network for the prototype model

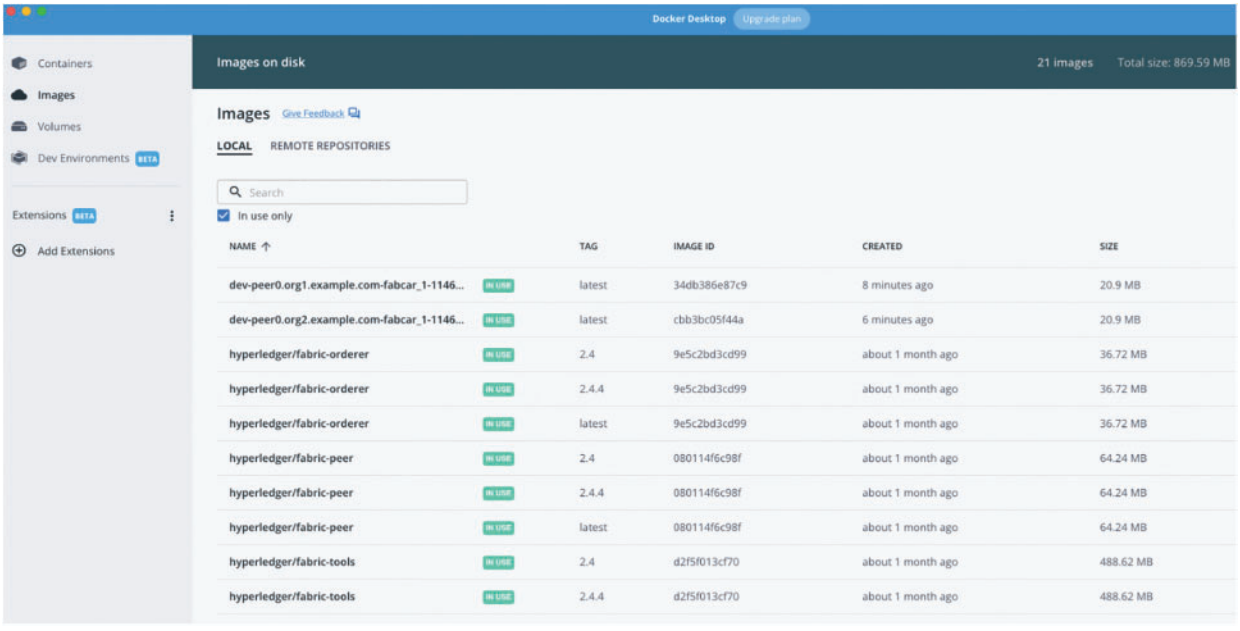

Figure 6: Blockchain deployment across a test network for the prototype model

The preparation of the dataset was performed as follows:

- First, nominal features were removed from all the dataset values. This was accomplished by dropping various columns that were not required for this study.
- All the null values were replaced with the help of the average value across cells to avoid any missing deals.
- All the labels available in the dataset were replaced with the help of a value ranging from [0, 1] using the scikit library.
- For better understanding, the binary classifiers were labeled 0 and 1 to indicate safe or attack, respectively.
- The normalization of all the values having higher resultant features was done with the help of scikit learn libraries in Python.
- The complete dataset was subdivided into five sub-datasets assumed to be data values on edge node devices. The partitioning was completed so that every client node was able to acknowledge intrusion or traffic anomalies.
- The testing and training division of the data was done at a scale of 80% to 20%. It was also checked that there is no redundant value existing between the testing and the training data set.

The feature selection from the dataset was made per the study proposed by [46]. The performance of the proposed system was enhanced with the help of the calculation of Shannon's joint entropy. As per the equation below:

$$Entropy = -\sum x \sum y \ (p\,(x, y) * \log_p (x, y) \tag{1}$$

The description of the features selected are:

The sequence number of the data packet = Seq

Number of inbound connections per source IP = n_Con_sIP

Number of inbound links per destination IP = n_Con_dIP

Packet clone from source to destination per second = sRate

Packet clone from destination to source per second = dRate

The minimum time taken in the records = Min

The maximum time for the records = Max

The average time is taken by the movement in the forms = Avg

The standard deviation amongst the forms = stdDev

A considerable entropy value represents randomness in the model. For all the features, the value of Shannon entropy was calculated as given by [47]. Next, the correlation between various features was calculated with the help of Pearson's coefficient. The output ranges from [−1, 1], and the value represents the degree of associativity between the features considered. A feature is ideal if it has high entropy and low correlation values. At the next stage, information gain for all the features was calculated with the help of the equation below:

$$InfoGain = Entropy\,(S) - \sum_1^k Pi * E\,(S,\ Qi) \tag{2}$$

The value of the information gain was collectively calculated for all the features, and the results are depicted in Fig. 7.

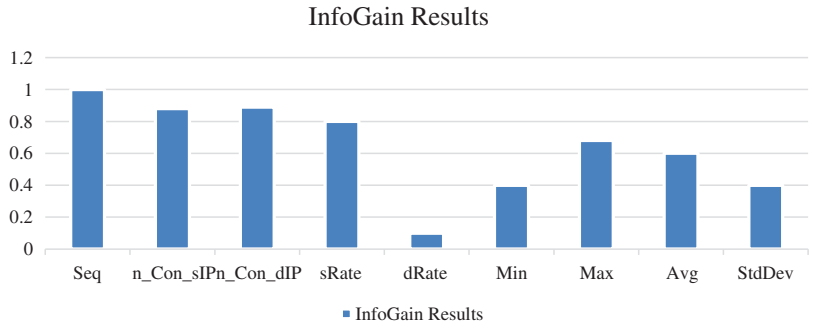

Figure 7: InfoGrain for all selected features for the proposed model

The features with better values for the information gained were taken into consideration and assessed for the suggested model. The evaluation of the model used for the detection of intrusion was done with the help of parameters: accuracy, precision rate, detection rate, the sensitivity of the model, specificity of the model, the value of the F1 score, and false alarm rate. A confusion matrix is created for the evaluation of the performance of the proposed model in the study given by [48]. Equation below represents a confusion matrix as per the equations below. This is helpful while evaluating the performance of a model using a machine-learning approach.

$$\text{Confusion Matrix} = \begin{bmatrix} TP & FN \\ FP & TN \end{bmatrix} \tag{3}$$

TP = True Positive TN = True Negative

FP = False Positive FN = False Negative

The calculation of the various parameters used to identify the effectiveness of this proposed study is done with the help of the following derivations given by [49] in Table 1.

Table 1: Calculation rules for the parameters used in the proposed study based on confusion matrix

Accuracy	$\frac{TP+TN}{TP+TN+FP+FN}$
Precision	$\frac{TP}{TP+FP}$
Recall	$\frac{TP}{TP+FN}$
Specificity	$\frac{TN}{TN+FP}$
F1 score	$\frac{2TP}{2TP+FP+FN}$
False alarm rate	$\frac{FP}{FP+FN}$

The testing of the dataset was done with the help of the features and the parameters stated in the above table. The binary classification for the model was done with the help of artificial neural networks. The machine learning model was assessed with two strategies comprising all the features selected in the model. The results are depicted in Table 2 below for the respective model evaluated for all and best features.

Table 2: ANN values for all features and best feature for the proposed model

ML parameters	Artificial neural network	
	All features	Best features
Accuracy	99.98%	99.98%
False alarm	11.01%	0.1%
Precision	99.99%	99.99%
Specificity	88.87%	99.99%
Recall	99.89%	99.88%
F1 score	99.98%	99.98%

A similar study for the experiment was conducted with the help of another algorithm called XGBoost. The results obtained from running a similar dataset with the parallel algorithm in comparison with the artificial neural network are depicted in Table 3.

Table 3: XGBoost values for all features and best feature for the proposed model

L parameters	XG-Boost algorithm	
	All features	Best features
Accuracy	98.40%	98.6%
False alarm	43.02%	42.18%
Precision	99.3%	99.2%
Specificity	56.89%	57.19%
Recall	99.3%	99.45%
F1 score	99.4%	99.4%

The general comparison between both algorithms reveals that the model proposed in this study is more efficient compared with the extant model. The intrusion detection is more likely to occur with the help of the proposed architecture in this study. The use of machine learning powers the detection procedure and is stronger when compared with the previous algorithms suggested by various other authors.

The Fig. 8 shows a comparison of training and testing data loss under the two algorithms. Both algorithms performed the training on the Bot-IoT dataset. Artificial neural networks have the tendency to learn from complex relationships for IoT applications [50]. Furthermore, this computing paradigm can learn from the initial data irrespective of the dataset and the distribution that has been used. The information coming from the IoT devices in healthcare units is best analyzed with the help of this proposed model. The quick and accurate prediction system proposed in this research makes

it suitable to be used by healthcare units. The ability of the model to identify intrusion and detect its occurrence is self-evident from the results recorded. This model is easily deployable and manageable for devices having limited processing capacity and low computational power. The IoT devices have smaller memory and less processing capability but can run the prescribed model to detect any intrusion early in the data processing and communication pipeline.

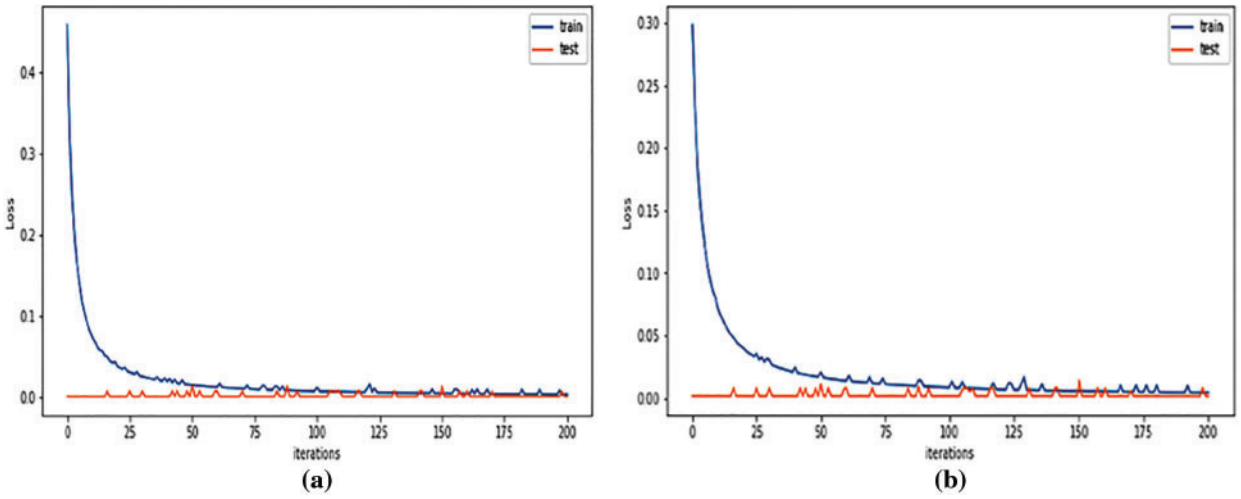

Figure 8: Training and testing loss for edge device (ANN and XGBoost algorithms) for Bot-IoT dataset

The intrusion detection model proposed in this study was initially evaluated with one dataset only. However, to validate the model with the help of different datasets, the same machine-learning algorithm was applied to different open-source datasets. The dataset reported in [51] comprised around 5 million records. These entries are network traffic-based details divided into four variant categories of attacks. Around 41 distinctive features were considered in this dataset related to the basic, traffic, and content-based information features. The dataset of [52] contained information related to network traffic. It comprises seven botnet types that are classified into various network features. Around 80 such features are available in this dataset. The dataset of [53] contained information and logs related to various internet-connected devices. The dataset is divided into seven botnet types for training purposes. This dataset comprises four distinct groups that contain various features based on the type, packet size, and behavior-oriented information. The test dataset comprises 16 botnet types, not in the training dataset. All the datasets considered for the model validation are open source and can be downloaded free from the referenced links.

The comparison of all the features represented in Table 4 indicates that the model proposed by this study performs well. With the help of machine learning algorithms implemented in the Python programming language, the average value for the training and testing loss at the edge gateway devices was analyzed. The results received from the analysis after the application of the machine learning algorithm were significant. Fig. 9 below compares the test and training dataset received after the model's training was completed.

Table 4: Comparison of parameters using multiple datasets

Datasets	CSE_CIC_IDS	BotNet-IoT	Bot-IoT (10 features)	Bot-IoT (All features)	KDD_Cup_99
Detection	0.4450	0.9990	1.0000	1.0000	0.9810
Sensitivity	0.8491	0.9452	0.9998	0.9998	0.9480
F1-score	0.5881	0.9870	0.9989	0.9998	0.9561
Specificity	0.8586	0.9995	0.9999	0.8887	0.9925
Accuracy	0.8578	0.9755	0.9999	0.9998	0.9844
Fake alarm rate	0.1450	0.0002	0.0001	0.0011	0.0068

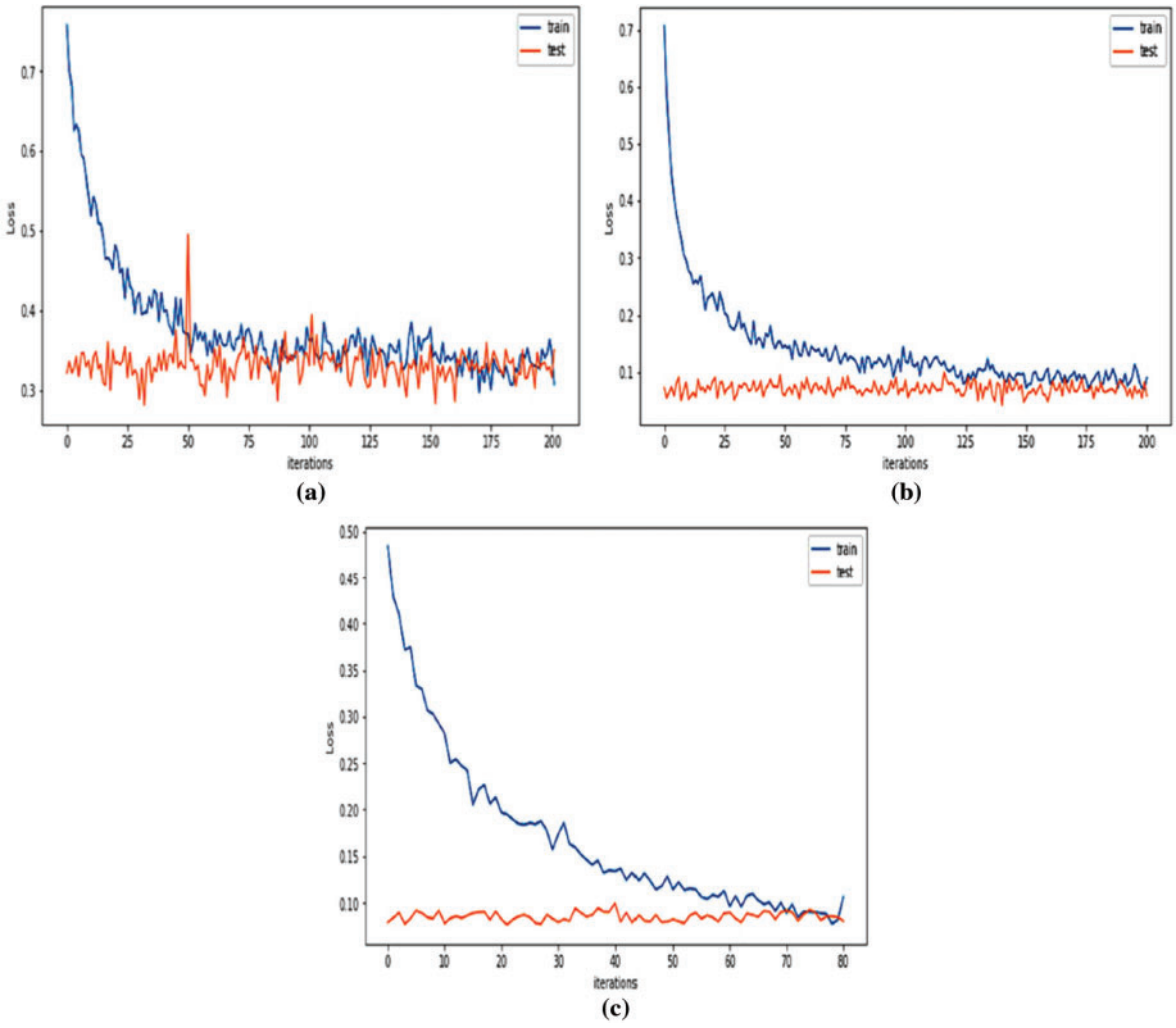

Figure 9: Average loss of the train and test data for the proposed model using the datasets [51–53]

5 Conclusion

In this paper, an intrusion detection mechanism was suggested for cloud-based applications that make use of IoT devices in healthcare units. The edge gateway devices send information to a blockchain network to ensure the secrecy and privacy of the data. Edge devices are becoming common in medical healthcare systems. The IoT devices used in medical settings are small units having low memory and minimal computational power. The proposed model can access information and identify any botnets. The edge devices take responsibility for intrusion detection, and the detection rules are updated at the edge server. Whenever an intrusion is detected at any of the edge devices, it immediately blocks the data from the gateway. Immediately after the intrusion is detected and blocked, the rules are updated inside the global edge server. These rules are posted to all the nodes inside the P2P network, which are responsible for sharing information. The data packets are trained with the help of training datasets and evaluated with the help of test datasets. For the training and testing of the model prescribed, three different datasets were considered, and the data was analyzed. The proposed architecture is useful for reducing intrusion and providing a mechanism that is useful for guarding against poisoning attacks. Various blockchain networks might face the problem of poisoning. The edge devices connected to the application server tend to upgrade the blocks across the P2P network. This ensures that the poisoning of any data block inside the chain does not occur. The detection of intrusion or poisoning is done with the secure cryptographic hash function. This cryptographic hash function is safe and cannot be changed unless operated without a smart contract. The exchange of contracts takes place between two peers after authorization with the help of the blockchain ledger. Despite the complexity of the Blockchain, it ensures the transparency and immutable nature of the information across the distributed and decentralized P2P network. The evaluation of the proposed model was done based on certain parameters using the Bot-IoT dataset. The results given by the prescribed model achieve an accuracy of 99.98%. A similar model was also assessed on three different datasets. As per the results, the proposed model gives the most accurate results in comparison with other existing models.

Acknowledgement: The authors extend their appreciation to the Deanship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work.

Funding Statement: The author extend their appreciation to the Deanship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the Project Number: IFP22UQU4400260DSR231.

Author Contributions: Jameel Almalki: Single Author Paper. Literature review, model design, experimental setup and design, data analysis, model training and results are all conducted by Jameel Almalki.

Availability of Data and Materials: Open-source dataset called BoT-IoT, created in a genuine environment in a Cyber-Security Lab at the University of New South Wales (UNSW). Availability of the Data Set: https://research.unsw.edu.au/projects/bot-iot-dataset.

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

References

[1] J. Almalki, W. Al Shehri, R. Mehmood, K. Alsaif, S. M. Alshahrani *et al.,* "Enabling blockchain with IoMT devices for healthcare," *Information*, vol. 13, no. 10, pp. 448, 2022.

[2] A. Alharbi and A. Rahman, "Review of recent technologies for tackling COVID-19," *SN Computer Science*, vol. 2, no. 460, pp. 1–27, 2021.

[3] S. D. Mamdiwar, Z. Shakruwala, U. Chadha, K. Srinivasan and C. Y. Chang, "Recent advances on IoT-assisted wearable sensor systems for healthcare monitoring," *Biosensors*, vol. 11, no. 10, pp. 372, 2021.
[4] V. M. Rohokale, N. R. Prasad and R. Prasad, "A cooperative internet of things (IoT) for rural healthcare monitoring and control," in *2nd Int. Conf. on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)*, Chennai, India, pp. 1–6, 2011.
[5] M. Alshamrani, "IoT and artificial intelligence implementations for remote healthcare monitoring systems: A survey," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 8, pp. 4687–4701, 2022.
[6] P. Sharma, M. D. Borah and S. Namasudra, "Improving security of medical big data by using blockchain technology," *Computers & Electrical Engineering*, vol. 96, pp. 107529, 2021.
[7] H. Li, X. Yang, H. Wang, W. Wei and W. A. Xue, "Controllable secure blockchain-based electronic healthcare records sharing scheme," *Journal of Healthcare Engineering*, vol. 2022, pp. 2058497, 2022.
[8] K. Azbeg, O. Ouchetto, S. J. Andaloussi and L. Fetjah, "A taxonomic review of the use of IoT and blockchain in healthcare applications," *IRBM*, vol. 43, no. 5, pp. 511–519, 2021.
[9] G. S. Aujla and A. Jindal, "A decoupled blockchain approach for edge-envisioned IoT-based healthcare monitoring," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 491–499, 2020.
[10] F. Aldosari, L. Abualigah and K. H. Almotairi, "A normal distributed dwarf mongoose optimization algorithm for global optimization and data clustering applications," *Symmetry*, vol. 14, no. 5, pp. 1021, 2022.
[11] I. Yaqoob, K. Salah, R. Jayaraman and Y. Al-Hammadi, "Blockchain for healthcare data management: Opportunities, challenges, and future recommendations," *Neural Computing and Applications*, vol. 34, no. 14, pp. 11475–11490, 2020.
[12] B. Shen, J. Guo and Y. Yang, "MedChain: Efficient healthcare data sharing via blockchain," *Applied Sciences*, vol. 9, no. 6, pp. 1207, 2019.
[13] F. Jamil, S. Ahmad, N. Iqbal and D. H. Kim, "Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals," *Sensors*, vol. 20, no. 8, pp. 2195, 2020.
[14] M. Sahoo, S. S. Singhar, B. Nayak and B. K. Mohanta, "A blockchain based framework secured by ECDSA to curb drug counterfeiting," in *10th Int. Conf. on Computing, Communication and Networking Technologies (ICCCNT)*, Kanpur, India, pp. 1–6, 2019.
[15] H. Xu, L. Zhang, O. Onireti, Y. Fang, W. J. Buchanan *et al.,* "BeepTrace: Blockchain-enabled privacy-preserving contact tracing for COVID-19 pandemic and beyond," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3915–3929, 2020.
[16] L. Yin, X. Luo, C. Zhu, L. Wang, Z. Xu *et al.,* "ConnSpoiler: Disrupting C&C communication of IoT-based botnet through fast detection of anomalous domain queries," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1373–1384, 2019.
[17] S. Walker-Roberts, M. Hammoudeh, O. Aldabbas, M. Aydin and A. Dehghantanha, "Threats on the horizon: Understanding security threats in the era of cyber-physical systems," *The Journal of Supercomputing*, vol. 76, no. 4, pp. 2643–2664, 2020.
[18] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein *et al.,* "Understanding the Mirai botnet," in *26th USENIX Security Symp.*, Vancouver, BC, Canada, pp. 1093–1110, 2017.
[19] N. Koroniotis, N. Moustafa and E. Sitnikova, "A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework," *Future Generation Computer Systems*, vol. 110, pp. 91–106, 2020.
[20] Y. Xiao, J. Wu, Z. Lin and X. Zhao, "A deep learning-based multi-model ensemble method for cancer prediction," *Computer Methods and Programs in Biomedicine*, vol. 153, pp. 1–9, 2018.
[21] S. M. Alshahrani, N. A. Khan, J. Almalki and W. Al Shehri, "URL phishing detection using particle swarm optimization and data mining," *Computers, Materials & Continua*, vol. 73, no. 3, pp. 5625–5640, 2022.

[22] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019.
[23] S. Mohapatra and S. Parija, "A brief understanding of IOT healthcare service model over remotely cloud connected environment," in *Advances in Intelligent Computing and Communication*, pp. 46–51, Singapore: Springer, 2020.
[24] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martinez-del-Rincon and D. Siracusa, "LUCID: A practical, lightweight deep learning solution for DDoS attack detection," *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 876–889, 2020.
[25] S. Latif, Z. Zou, Z. Idrees and J. Ahmad, "A novel attack detection scheme for the industrial internet of things using a lightweight random neural network," *IEEE Access*, vol. 8, pp. 89337–89350, 2020.
[26] Z. Chen, N. Lv, P. Liu, Y. Fang, K. Chen *et al.,* "Intrusion detection for wireless edge networks based on federated learning," *IEEE Access*, vol. 8, pp. 217463–217472, 2020.
[27] F. Lin, Y. Zhou, X. An, I. You and K. K. R. Choo, "Fair resource allocation in an intrusion-detection system for edge computing: Ensuring the security of internet of things devices," *IEEE Consumer Electronics Magazine*, vol. 7, no. 6, pp. 45–50, 2018.
[28] G. W. Cassales, H. Senger, E. R. de Faria and A. Bifet, "IDSA-IoT: An intrusion detection system architecture for IoT networks," in *IEEE Symp. on Computers and Communications (ISCC)*, Barcelona, Spain, pp. 1–7, 2019.
[29] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider and M. Hamdi, "A survey on security and privacy issues in edge-computing-assisted Internet of Things," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4004–4022, 2022.
[30] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y. C. Liang *et al.,* "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 2031–2063, 2020.
[31] S. Wang, T. Tuor, T. Salonidis, K. K. Leung, C. Makaya *et al.,* "Adaptive federated learning in resource constrained edge computing systems," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 6, pp. 1205–1221, 2019.
[32] S. Agrawal, S. Sarkar, O. Aouedi, G. Yenduri, K. Piamrat *et al.,* "Federated learning for intrusion detection system: Concepts, challenges and future directions," *Computer Communications*, vol. 195, no. 1, pp. 346–361, 2022.
[33] H. B. McMahan, E. Moore, D. Ramage and B. A. Y. Arcas, "Federated learning of deep networks using model averaging," arXiv preprint arXiv:1602.05629, pp. 1–11, 2016.
[34] Y. Zhao, J. Chen, D. Wu, J. Teng and S. Yu, "Multi-task network anomaly detection using federated learning," in *Proc. of the 10th Int. Symp. on Information and Communication Technology*, Hanoi, Vietnam, pp. 273–279, 2019.
[35] S. Rajendran, J. S. Obeid, H. Binol, K. Foley, W. Zhang *et al.,* "Cloud-based federated learning implementation across medical centers," *JCO Clinical Cancer Informatics*, vol. 5, pp. 1–11, 2021.
[36] N. Rieke, J. Hancox, W. Li, F. Milletari, H. R. Roth *et al.,* "The future of digital health with federated learning," *NPJ Digital Medicine*, vol. 3, no. 1, pp. 1–7, 2020.
[37] K. Peter, H. B. McMahan, A. Brendan, B. Aurélien, B. Mehdi *et al.,* "Advances and open problems in federated learning," *Foundations and Trends in Machine Learning*, vol. 14, no. 1–2, pp. 1–210, 2021.
[38] T. D. Nguyen, P. Rieger, M. Miettinen and A. R. Sadeghi, "Poisoning attacks on federated learning-based IoT intrusion detection system," in *Proc. of Workshop Decentralized IoT Systems and Security (DISS)*, San Diego, CA, USA, pp. 1–7, 2020.
[39] E. Bagdasaryan, A. Veit, Y. Hua, D. Estrin and V. Shmatikov, "How to backdoor federated learning," in *Int. Conf. on Artificial Intelligence and Statistics*, Palermo, Italy, pp. 2938–2948, 2020.

[40] J. Zhang, J. Chen, D. Wu, B. Chen and S. Yu, "Poisoning attack in federated learning using generative adversarial nets," in *18th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications/13th IEEE Int. Conf. on Big Data Science and Engineering (TrustCom/BigDataSE)*, Rotorua, New Zealand, pp. 374–380, 2019.
[41] O. Alkadi, N. Moustafa, B. Turnbull and K. K. R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9463–9472, 2020.
[42] S. Aldhaheri, D. Alghazzawi, L. Cheng, B. Alzahrani and A. Al-Barakati, "DeepDCA: Novel network-based detection of IoT attacks using artificial immune system," *Applied Sciences*, vol. 10, no. 6, pp. 1909, 2020.
[43] T. T. Huong, T. P. Bac, D. M. Long, B. D. Thang, N. T. Binh *et al.,* "Lockedge: Low-complexity cyberattack detection in IoT edge computing," *IEEE Access*, vol. 9, pp. 29696–29710, 2021.
[44] A. Shenfield, D. Day and A. Ayesh, "Intelligent intrusion detection systems using artificial neural networks," *IoT Express*, vol. 4, no. 2, pp. 95–99, 2018.
[45] L. P. Dias, J. D. J. F. Cerqueira, K. D. Assis and R. C. Almeida, "Using artificial neural network in intrusion detection systems to computer networks," in *9th Computer Science and Electronic Engineering (CEEC)*, Colchester, UK, pp. 145–150, 2017.
[46] N. Koroniotis, N. Moustafa, E. Sitnikova and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," *Future Generation Computer Systems*, vol. 100, pp. 779–796, 2019.
[47] A. Lesne, "Shannon entropy: A rigorous notion at the crossroads between probability, information theory, dynamical systems and statistical physics," *Mathematical Structures in Computer Science*, vol. 24, no. 3, pp. e240311, 2014.
[48] H. M. Balaha, M. Saif, A. Tamer and E. H. Abdelhay, "Hybrid deep learning and genetic algorithms approach (HMB-DLGAHA) for the early ultrasound diagnoses of breast cancer," *Neural Computing and Applications*, vol. 34, no. 11, pp. 8671–8695, 2022.
[49] G. A. Mohamed, E. H. Abd El Hay, I. Y. Abdel-Baset and M. M. Abd El Azim, "Development machine learning techniques to enhance cybersecurity algorithms," *Mansoura Engineering Journal*, vol. 46, no. 4, pp. 36–46, 2021.
[50] K. Suzuki, *Artificial neural networks: Methodological advances and biomedical applications*, 1st ed., London, UK: InTechOpen Limited, 2011.
[51] S. Stolfo, W. Fan, W. Lee, A. Prodromidis and P. Chan, "Cost-based modeling and evaluation for data mining with application to fraud and intrusion detection: Results from the JAM project," Columbia University, pp. 1–16, 1999. [Online]. Available: http://ids.cs.columbia.edu/sites/default/files/ada511232.pdf
[52] I. Sharafaldin, A. Habibi Lashkari and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Int. Conf. on Information Systems Security and Privacy (ICISSP 2018)*, Funchal, Madeira, Portugal, pp. 108–116, 2018.
[53] I. Sharafaldin, A. Habibi Lashkari, S. Hakak and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," in *IEEE 53rd Int. Carnahan Conf. on Security Technology*, Chennai, India, pp. 1–8, 2019.