ISSN 2320 - 2602

Volume 13 No. 7, July 2024

International Journal of Advances in Computer Science and Technology

Available Online at http://www.warse.org/IJACST/static/pdf/file/ijacst021372024.pdf

https://doi.org/10.30534/ijacst/2024/021372024

A Hybrid Machine Learning Approach for Intrusion Detection and Mitigation on IoT Smart Healthcare

Eterigho Okpomo Okpu[1], Onate Egerton Taylor[2], Nuka Dumle Nwiabu[3], Daniel Matthias[4]

[1] Department of Cyber Security, Delta State University of Science & Technology, Ozoro, Nigeria, okpuoe@dsust.edu.ng

[2] Department of Computer Science, Rivers State University, Port-Harcourt, Nigeria, taylor.onate@ust.edu.ng

[3] Department of Computer Science, Rivers State University, Port-Harcourt, Nigeria, nwiabu.nuka@ust.edu.ng

[4] Department of Computer Science, Rivers State University, Port-Harcourt, Nigeria, matthias.daniel@ust.edu.ng

Received Date : May 28 , 2024 Accepted Date : June 29, 2024 Published Date : July 07, 2024

ABSTRACT

Strong cybersecurity solutions are becoming more and more important as Internet of Things (IoT) technology integration in healthcare settings develops. This study offers a method for feature extraction, selection, and attack classification by fusing the discriminative capacity of feedforward neural networks (FNNs) with the adaptability of fuzzy logic systems. In delicate healthcare database of IoT wearable devices, to reduce false alarm and guaranteeing intrusion detection dependability are the main priorities. The suggested method uses a feature extraction, selection technique, training and testing based on FNN, which allows the model to adjust to the dynamic and varied character of medical data. During the assessment stage, a dataset including a range of healthcare IoT scenarios, including different kinds of attacks, is used to train and evaluate the model, the ToN_IoT dataset was used. Fuzzy logic improves the system's resilience in identifying pertinent features by managing uncertainties and imprecise input. Fuzzy logic is one of the best technique for handling uncertainty, its linguistic representation and rule reasoning helps in better identification and classification. The findings indicate a noteworthy decrease in the frequency of false alarms when juxtaposed with conventional intrusion detection systems. Results obtained from the model are 99.2, 98.8, 99.5, 99.1 & 0.008 for accuracy, precision, recall, F1-Score and False alarm respectively. Promising outcomes in protecting IoT healthcare environments are demonstrated by the suggested system, opening the door to better patient data privacy and system resilience against cyberattacks.

Key words : Intrusion Detection System (IDS); Internet of Things (IoT); Internet of Medical Things (IoMT); Feedforward Neural Networks (FNN); Fuzzy Logic System; wearable device manometer; Man-in-the-middle attack (MitM); Distributed Denial of Service (DDoS) attack; Ransomware.

1. INTRODUCTION

The recent development in mobile technology has improved the connectivity amongst people across the globe making it easy for government, businesses and individuals to interact and engage seamlessly in actual time. The Internet of Things (IoT) makes universal communicating infrastructure between humans and machines easy and secured using intrusion detection system (IDS) security [1]. IoT builds a global infrastructure that will transform many facets of our life, including manufacturing, mining, agriculture, and health care. The implementation of internet of things in the healthcare region promises a new lease of life to healthcare delivery as it improves the services and activities of the healthcare sector in terms of patients and processes related procedures with respect to scarce human and medical resources [2]. A wearable device manometer could be utilized in the medical industry to continually measure blood pressure throughout the day, giving an extra thorough picture of a patient's cardiovascular health [3]. Some instances of wearable Internet of things (IoT) medical devices are continuous glucose monitors, Smart Clothes, Wearable ECG monitors, Smart Watches, Wearable Respiratory Monitors etc [4].

Attacks on internet-connected and enabled medical devices have the prospective to cause major emotional, physical harm and even death to patients. More and more challenges emerge on daily basis from the healthcare IoT environment which tends to impede and compromise the efficiency of the system with respect to health information management and security concerns. Common IoT attacks are the sinkhole attack, the wormhole occurrence, Man-in-the-middle attack (MitM), Distributed Denial of Service (DDoS) attack, Eavesdropping, Ransomware and much more [5][6]. According to estimates, medical organizations will have to pay $15.5 million in 2023 for the downtime caused by assaults [7]. With 6,248 DDoS Attacks in the healthcare industry in 2022, DDoS attacks have dominated incidences. In the second quarter of 2023, there was a fifteen percent rise in application-layer DDoS attacks [8].

According to [9], in 2018, there were 2216 privacy-related complaints from 65 countries. Of these, 536 led to security breaches in the healthcare industry. In [9], this indicates that the healthcare industry has seen the most number of breaches across all industries.

There is therefore the urgent need to protect and secure this key resource from malevolent users and intruder who pry to steal and alter such information for their own good. One security measure for identifying attacks is the intrusion detection system (IDS) [10]. It is a collection of methods for identifying questionable activity at the host and network levels [11]. IDSs can be divided into two primary groups, according to [12]: "Signature based," which recognizes harmful patterns. Although a signature-based intrusion detection system (IDS) has a low false alarm rate and excellent accuracy, it cannot identify brand-new threats [13]. "Anomaly-based" is the other type that makes a distinction between deviations. Because anomaly-based IDS can identify novel assaults, they are favored over signature- and specification-based IDS; nevertheless, this comes at an elevated false alarm rate [14]. Most existing systems cannot clearly identify attack and also misclassify the type of attack. Most of the present systems have great rate of false alarm which will lead to damage in trust and reliability of the system. False alarm can also lead to fear, disruption of emergency services, and waste of resources in wearable manometer.

In this research, based on the above mentioned issues, the researchers developed an improved intrusion detection system which will monitor, detect, mitigate and reduce false alarm rate using hybrid machine learning method. The objectives of the study develop an artificial neural network technique for training and testing the model and utilize Fuzzy Logic system to clearly identify the type and classify attack, which will reduce the false alarm rate. The model was implemented with python programming language. The scope of this research is to develop an intrusion detection system for IoT-based database healthcare for wearable manometer blood pressure devices, Smart watches wearable, Fitness tracker, Temperature Sensor devices and Smart Clothes information monitoring for Hypertension disease. The types of attacks considered in this study are Man in the middle, DDos and Ransomware.

2. LITERATURE REVIEW

2.1 Artificial Neural Network

A model of the human brain is an artificial neural network (ANN). The brain has the most extraordinary ability to interpret ambiguous, hazy, and incomplete information and draw its own conclusions from it [15]. Artificial neurons are connected in a way that is comparable to the brain network in an imitation neural network, or ANN. They are made up by layer-organized, networked nodes, or neurons. Every neuron receives incoming signals, uses an activation function to process them, and then produces an output signal that it can send to other neurons. Applications for them can be found in many different fields, including as robotics, finance, healthcare, natural language processing, image and audio recognition, and more. Many architectures, including feedforward, recurrent, and convolutional networks, have been developed to efficiently handle many kinds of tasks [16]. One of the most basic and straightforward structures in the field of artificial neural networks is a feedforward neural network (FNN). Each layer is completely connected to the one above it, and it is made up of several layers of interconnected neurons. The word "feedforward" refers to the direction in which information flows: from the input layer to the output layer via one or more hidden layers.

2.2 Fuzzy Logic

A multivalued logic known as fuzzy logic (FL) enables the definition of intermediate values between traditional assessments such as true/false, yes/no, high/low, etc. In order to bring a more human-like way of thinking to the programming of computers, concepts like fairly tall or very fast can be formally expressed and processed by computers [17]. A fuzzy logic system (FLS) is defined as a nonlinear mapping of an input data (feature) vector into a scalar output (the vector output case decomposes into a group of independent multi-input/ single-output systems), according to [18]. There are typically three stages in fuzzy logic. The Actual value is a system input during the fuzzification process. Each input value undergoes transformation and membership rating. In the second stage, algorithm rules are provided. The rule table is changed to fit the input [19]. Defuzzification, the final stage, involves converting fuzzy values to actual values [20].

2.3 Fuzzy Logic

Remote patient monitoring has improved since the Internet of Medical Things (IoMT) was introduced. It lessens the load on health care systems and the number of needless hospital visits by establishing a connection between patients and their doctors and enabling the transmission of health data across a secure network [21]. Healthcare providers can obtain patient biometrics in real time, monitor patients' vital signs from a distance, and stay on top of any possible problems to help prevent further complications. By enabling individuals to transmit health information data to physicians, IoMT offers the potential to reduce healthcare expenditures, increase accuracy of diagnoses, and reduce errors through the use of technology [22]. [23] Asserts that as the need for ways to reduce healthcare expenses grows in the next years, the IoMT is set to revolutionize how we preserve people safe and well. A wearable manometer which is worn on the body could be utilized in the medical industry to continually measure blood pressure throughout the day, giving an extra thorough picture of a patient's cardiovascular health [3]. Numerous devices, including smart watches, smart glasses with optical sensors built in, circuit boards strapped to our abdomens, wearable devices that fit on our fingers, and discreetly connected sensors to our hands, arms, and chests, are examples of blood pressure wearables [24]. The medical services context can be expanded by the system from the patient's home to the physician's office [25]. [4] While medical professionals can keep an eye on patients at predetermined intervals, health problems can strike at any time, necessitating continuous vital sign monitoring.

Figure 1 displays wearable technology-based blood pressure monitoring devices.

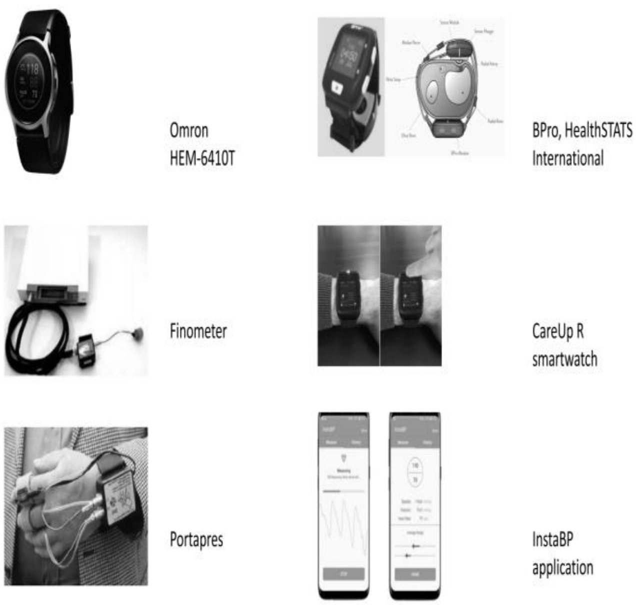


Figure 1: Wearable Devices used for Blood Pressure Measurement, using various Technology health [3].

A wearable IoT manometer that is specifically made for taking blood pressure is a gadget that integrates IoT capabilities with manometer functionality to give continuous, linked blood pressure monitoring [26].

2.4 Review of Related Works

[27] Examined several deep learning (DL) techniques for intrusion detection systems (IDSs) in the Internet of Things (IoT) and the related datasets in order to identify gaps, vulnerabilities, and a neutral reference design. Along with a comparison of IDSs, a review of anomaly-based IDSs using DL approaches, including supervised, unsupervised, and hybrid methods, is given. The majority of the methods used in these three categories have been implemented in Internet of Things settings. Thus far, anomaly-based IDS for IoT has only employed a small number of them. For each of these anomaly-based IDSs, the application of the four feature(s) extraction, classification, prediction, and regression was assessed while important performance metrics and benchmark detection rates were examined, along with the necessary effectiveness of the different techniques. Four machine learning algorithms-LR, SVM, DT, and ANN—were assessed for classification purposes.

The Multi-Feature Extraction Extreme Learning Machine (MFE-ELM) technique was placed on cloud nodes in order to find and detect network breaches. This technique enhances cloud servers with a multi-feature extraction process. For testing in the simulation trials, a standard intrusion detection dataset is selected, and test methods including feature engineering, data preprocessing, model training, and result analysis are conducted. The trials' results show that the recommended technique can effectively recognize and identify most network data packets while preserving high model execution times [28].

A methodology for designing micro-IDSs with small false positive and false negative rates to identify attacks on IoT and networking protocols was developed by [29]. They created brand-new, unique data structures that we call n-grams and observation flows, which were utilized to precisely describe the typical behavior of the networking protocol and Internet of Things. Additionally, the researchers created intrusion detection systems that are very correct in identifying assaults against the HTML, DNS, and Wi-Fi protocols.

The goal of [30] is to improve industrial IoT cybersecurity by using intrusion detection on the network traffic that is generated. Utilizing the source and destination payload lengths as well as the connection states specified in Zeek logs, a lightweight intrusion detection technique built on the Markov model was put forth. Using the empirical probability law and Hellinger distance, the researchers were able to identify intrusive network traffic with a high degree of accuracy.

A novel mobile agent based IDS was designed and developed by [31] to protect the network of connected medical devices. To be more precise, the suggested system is hierarchical and autonomous, and it makes use of machine learning and regression methods to find anomalies in sensor data as well as network level intrusions. The simulation's results demonstrate that they can achieve high detection accuracy with minimal resource overhead.

This paper proposes an SDN-based intrusion detection framework using machine learning techniques. SDN is a method that enables software applications to be used to centrally and intelligently operate a network. Within its architecture, the SDN controller generates intrusion alarms by watching the behavior of industrial IoT devices using a machine-learning algorithm. According to the results, the proposed framework can identify attacks on industrial IoT networks and devices with 99.7% accuracy [32].

Modern IoT network security protocols and network intrusion detection systems (NIDS) were thoroughly examined by [33]. The authors applied machine learning (ML) techniques and MEC platforms to a number of tactics, which were thoroughly analyzed. The research piece also examines the publicly available datasets utilized in NIDS design, as well as deployment strategies and evaluation metrics. Lastly, the authors propose an IoT network NIDS framework based on MEC.

With a 96% accuracy rate, the B-GNB model shows a high degree of precision in classifying different types of attacks in health care IoT data. When it comes to efficiently identifying a broad variety of threats, the B-GNB model outperforms more established techniques like GNB and RF classifiers. The study made use of the 477,426 data points in the Open-Source IoT Device Network Logs dataset, which had 13 input attributes and one output label class called normalcy. The methodology that has been suggested includes a classification system that allocates a certain set of attributes and point values to every kind of attack [34].

For the objective of identifying unauthorized access in smart healthcare systems (SHS), machine learning methods can be used with success. The healthcare industry has benefited immensely from the amalgamation of wearable devices and Internet of Things (IoT) sensors in smart healthcare systems (SHS). This has allowed for prompt medical treatments and reduced hospitalization costs. With an accuracy rate of 95%, the AdaBoost classifier has shown encouraging results in identifying network intrusion within SHS [35].

The research proposes three deep learning (DL) models—LinSVM, ConvSVM, and CatEmbedding—for the secure intrusion detection system (IDS) design and implementation on the IoMT network. This article also evaluates different machine learning (ML) techniques for intrusion detection in the IoMT ecosystem. Five of the seven machine learning models that were suggested—LR, RF, DT, XGBoost and GradBoost—achieved a 100% accuracy rate, while SVM and KNN yielded 99.9% and 99.8% accuracy rates, respectively. ConvSVM was shown to converge to 0 more quickly than the other two models after 50 epochs [36].

3. METHODOLOGY

The combination of the fuzzy system and the deep neural network model is aimed at the reduction of the noise and imprecision in the existing system thereby generating a better and more accurate intrusion detection and classification process in the medical IoT environment. Training and testing of the dataset is done by the FNN while the fuzzy system will be used for the Identification and classification process. Figure 2 shows architecture of the neural network FNN model and fuzzy logic for intrusion detection. In Figure 3, the compressed version of the architecture was revealed. In Figure 2, it shows the number of hidden layers, activation function used. Table 1 displays the different paremeters used in the FNN. The architecture of the suggested system in Figure 4 displays an improvement on the existing system architecture and with the addition of the IoT devices and the fuzzy logic component to the existing model which enables it to effectively detect and classify intrusion agents from the datasets. The trained FNN model is prepared to categorize incoming network traffic using the features it has acquired during training. The technique for identifying attacks is the fuzzy logic. A Fuzzy Logic system processes the features taken out of the fresh network traffic and uses the trained FNN model to assess whether the traffic is indicative of an intrusion or normal behavior.

The proposed system comprises a broad category of systems that combines to form the IoT Healthcare system using wearable devices. The system consists of IoT medical wearable manometer blood pressure devices, Smart watches wearable, Fitness tracker, Temperature Sensor devices and Smart Clothes information monitoring for Hypertension disease which are connected to the IoT healthcare services and a Hybrid Machine Learning Intrusion Detection System (IDS) which consist of deep neural network model and fuzzy inference systems. In the proposed system, Database will be protected using the Hybrid Machine Learning IDS which will check the network traffic data using the fuzzy logic system and with its rules and the trained FNN model will detect and classify if there is an intrusion or not. If there is an intrusion, the system will block the node, and when there is no intrusion which means the node is normal and it will be allowed to communicate with database.

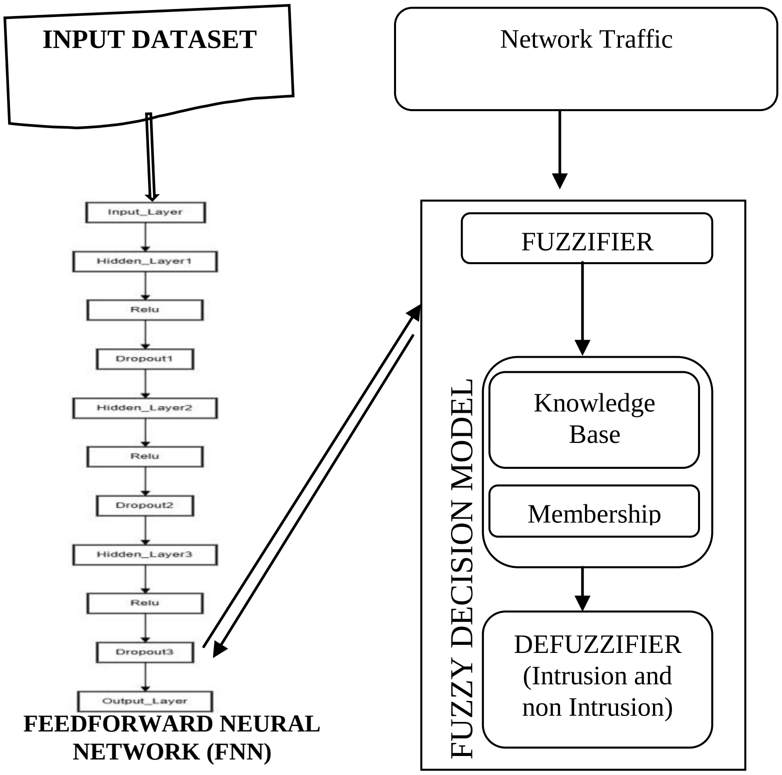


Figure 2: Architecture of the FNN and Fuzzy Logic

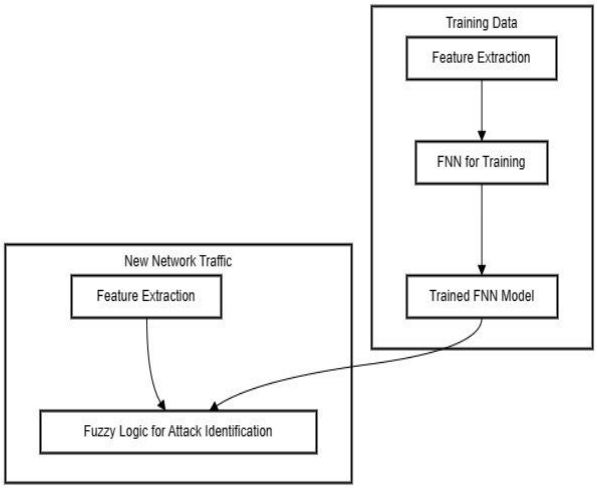


Figure 3: Compressed System Architecture

Table 1: Parameters for Training FNN

Parameter	**Description**	**Example Values**
Number of Hidden Layers	The neural network's total amount of hidden layers.	1, 2, 3
Neurons per Hidden Layer	The quantity of units, or neurons, in every buried layer.	64, 32, 16
Activation Functions	The neurons in the hidden layers are subjected to the activation functions.	ReLU
Learning Rate	The speed at which the network's weights are changed during training.	0.01
Batch Size	How many training examples are used in each training cycle.	128
Optimizer	The optimization technique that updates the network's weights while it is being trained.	Adam
Initialization Method	The process by which the network's weights are initialized.	Random
Number of Epochs	The amount of times the neural network is trained by passing the complete training dataset both forward and backward.	100
Momentum	a parameter that optimization algorithms employ to get around oscillations and speed up convergence.	0.9

In Figure 4 it illustrates the Architecture of the Proposed Deep Neuro-Fuzzy System for IoT Healthcare. The purpose of monitoring the data produced by IoT devices in the smart healthcare system is shown by the diagram labeled "Monitor Device Data." Create Feedforward Neural Network: For the purpose of training and testing the intrusion detection dataset, a feedforward neural network approach is being developed. Use a Fuzzy Logic System: In this instance, the assault type is identified and classified with clarity through the usage of a fuzzy logic system. With the ultimate objective of leveraging both the neural network and fuzzy logic system to improve the intrusion detection and mitigation capabilities of the IoT smart healthcare system, each succeeding scenario builds upon the one that came before it.

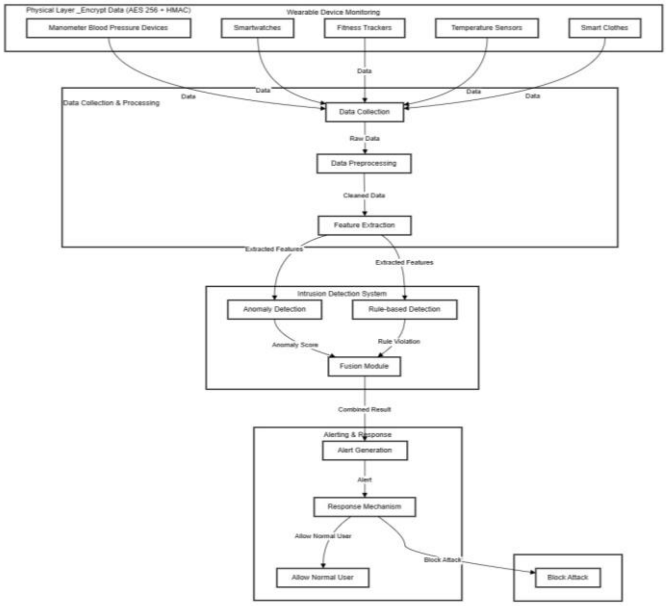


Figure 4: Architecture of the Proposed Deep Neuro-Fuzzy System for IoT Healthcare

3.1 Algorithm of the Proposed System

1. Upload Dataset
2. Initialization
3. Forward Propagation
4. Softmax Activation
5. Loss Computation
6. Backpropagation
7. Repeat
8. Duplicate steps 2-5 for a fixed amount of epochs or until convergence standards are met End if output matches the target or desired alert
9. Procedure Fuzzy Inference System(inputs: list of crisp input values):
10. Fuzzification
11. For each input variable i
12. For each linguistic term j of variable i
13. Calculate membership grade μ_{ij} using corresponding membership function
14. Rule Evaluation
15. For each rule r
16. Evaluate the antecedent of rule r to determine its firing strength
17. Aggregation
18. Combine the firing strengths of all rules to obtain a single fuzzy output
19. Defuzzification
20. Calculate the crisp output value using defuzzification method
21. Return crisp output value
22. Classify target output as intrusion alert and block the intrusion

```
23.  Else
24.  Classify target as negative
```

3.2 Dataset

ToN_IoT is the dataset used for the suggested system. For IoT/IIoT applications, this is one of the most recent datasets. In 2019, the Cyber Range and IoT Labs at the University of New South Wales in Australia gave a presentation on it. This is an extremely helpful dataset for assessing the fidelity and effectiveness of various ML/DL-based cybersecurity systems. There are 1379274 samples in the ToN_IoT total; of these, 270279 are considered normal samples while 1108995 are considered aberrant values. In Table 2 the Dataset used for the system was shown.

Table 2 ToN_IoT Dataset

S/N	Feature	Description
1	IPV4_SRC_ADDR	IPv4 source address
2	IPV4_DST_ADDR	IPv4 destination address
3	L4_SRC_PORT	IPv4 source port number
4	L4_DST_PORT	IPv4 destination port number
5	PROTOCOL	IP protocol identifier byte
6	L7_PROTO	Layer 7 protocol (numeric)
7	IN_BYTES	Incoming number of bytes
8	OUT_BYTES	Outgoing number of bytes
9	IN_PKTS	Incoming number of packets
10	OUT_PKTS	Outgoing number of packets
11	FLOW_DURATION_MILLISECONDS	Flow duration in milliseconds

3.3 Data Preprocessing

Pre-processing comes next after data collection, and our model is then trained using the pre-processed data. The data is cleaned, converted, divided into training and testing sets. A CSV file containing 43 NetFlow functions, each with an outbreak class and a label indicating whether it is harmful or benign. Technique used for data reprocessing are filling in missing numbers, reducing noise in the data, locating and eliminating outliers, and resolving discrepancies are all steps in the data cleaning process. The technique for reducing data is dimensionality reduction. Reducing the amount of random variables or attributes under consideration is known as dimensionality reduction. The data transformation method that will be used is called normalization, and it involves scaling the attribute values to fall into a more constrained range, such as -1.0 to 1.0 or 0.0 to 1.0. Value magnitudes are scaled to noticeably low values during normalization. Min-max normalization is the most widely used technique for this scope.

4.0 EVALUATION METRICS

1. True Positive (TP): Accurately identified data points
2. True Negative (TN): Data points that are accurately categorized as not falling under a specific type
3. False Positive (FP): When data sets misclassify one class as the proper class, this is known as false positive (FP).
4. False Negative (FN): Data points that were misclassified as belonging to a different class.
5. Accuracy (A) is the fraction of forecasts our model got right.
6. Precision indicates the proportion of samples in the positive class among those the model classified as being in the positive class.
7. Recall (R) of a class is the fraction of correctly classified out of all that actually belong to that class.
8. F1- Score, is the harmonic mean of recall and precision.

5.0 RESULTS AND DISCUSSION

In our proposed model dashboard, model we monitor different IP addresses coming into the system and block an IP address with intrusion shown in Figure 5. An instance of MitM attack is revealed in Figure 6. The dashboard of the proposed system shown in figure 5 shows how the system monitors, detect and mitigate intrusion on the network. The system can be set to manual monitoring or automatic monitoring. In manual monitoring, the user of the system will have to block and quarantine node that are doubtful in the network manually. While the automatic monitoring, the system on its own block and quarantine node that are uncertain in the network. On the dashboard, there is list of ip addresses on the network. In figure 6, is the demonstration of how the system detected MitM. The ip address of the node carrying the attack is also displayed.

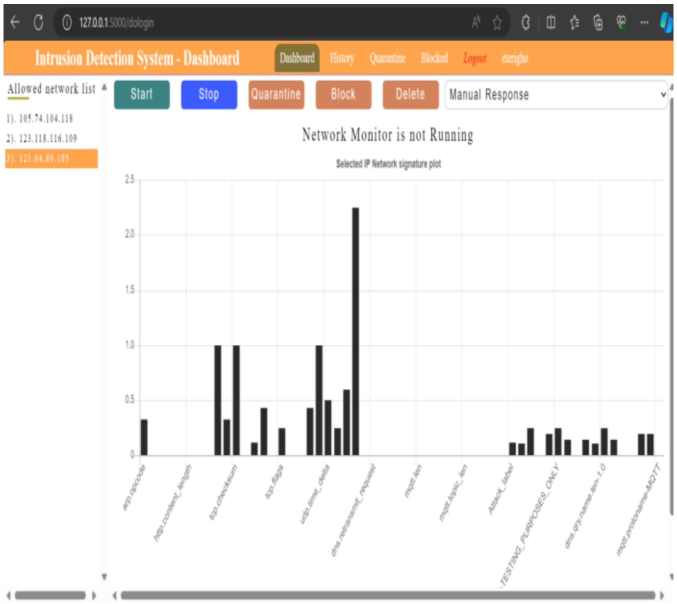
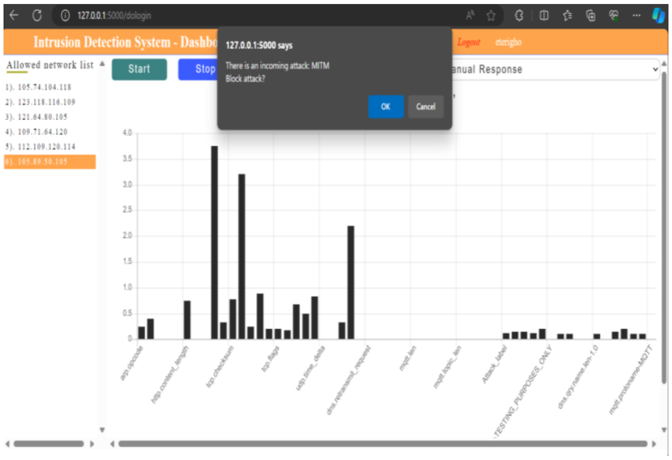


Figure 5: Dash board of the proposed system



127.0.0.1:5000/dologin

Intrusion Detection System - Dashbo

127.0.0.1:5000 says

There is an incoming attack: MITM
Block attack?

Allowed network list

1). 105.74.104.118
2). 123.118.116.109
3). 121.64.80.105
4). 109.71.64.120
5). 112.109.120.114
6). 105.89.50.105

Figure 6: Man in the middle attack

In Table 3, details of ip addresses that are man-in-middle, DDoS, Ransomware attacks, normal user and quarantine were shown. In Table 3, it shows number of ip addresses of different attacks that were predicted right and the number ip addresses that were predicted wrongly. It also illustrates the numbers of ip addresses that were predicted normal user in the system. Table 4 proves result of the proposed system testing with TON_IoT dataset.

Table 3: Analysis of Result

Attacks/ Normal user	No. of ip addresses Correctly predicted	No. of ip addresses wrongly predicted	No. of ip addresses
Man-in-the-Middle	**150**	**1**	**151**
DDoS	**191**	**1**	**192**
Ransomware	**282**	**2**	**284**
Normal	**699**	**3**	**702**
Quarantine			**3**
Total			**1332**

In Figure 7 the confusion matrix of the proposed system was exposed. In Figure 7, this presents the predicted results and the actual results. It shows that True Positives (TP) is 623, False Positives (FP) is 3, True Negatives (TN) is 699 and False Negatives (FN) is 7 when 1332 ip addresses where checked. In Table 5, the classification models performance Metrics was demonstrated. In Figure 8 Performance Evaluation Graph of the suggested system was revealed,

Table 5: Classification Models Performance

	Accuracy	**Precision**	**Recall**	**F1-Score**	**False alarm**
Models	99.2	98.8	99.5	99.1	0.008 %

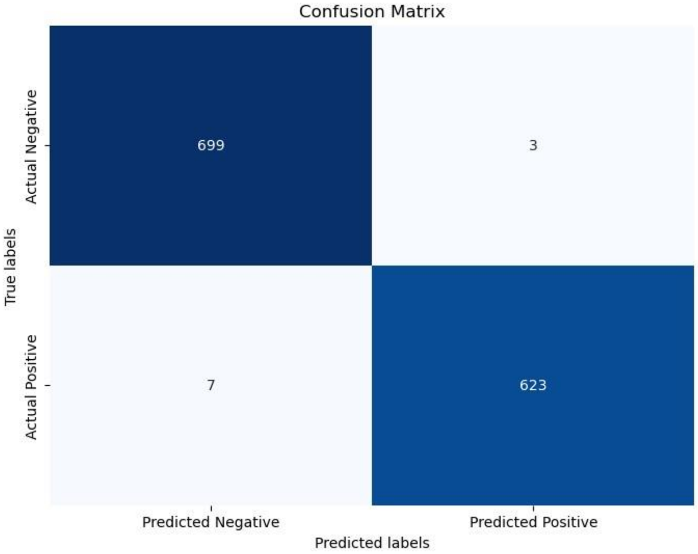


Figure 7: Confusion matrix of the proposed system for detection

Table 4: Results of the proposed system testing using ToN_IoT

N/S	**Source IP_Addresses**	**Destination IP_Addresses**	**Source Port**	**Destination Port**	**Protocol**	**Outcome**	**Recommendations**
1	192.168.1.46	192.0.0.251	5353	5353	Udp	Normal	Allow
2	192.168.1.30	172.16.1.19	34190	80	Tcp	DDos	Block
3	192.168.1.193	10.16.1.37	49236	4444	Tcp	Ransomware	Block
4	112.79.65.115	115.168.1.190	1880	51782	Tcp	Normal	Allow
5	108.90.59.105	112.16.1.16	5	1	Icmp	Mitm	Block
6	103.112.51.103	10.16.1.19	4444	49235	Tcp	Ransomware	Block
7	172.1.1.60	192.168.1.1	51422	53	Udp	DDos	Block
8	10.10.12.11	102.16.10.1	52016	53	Udp	Mitm	Block

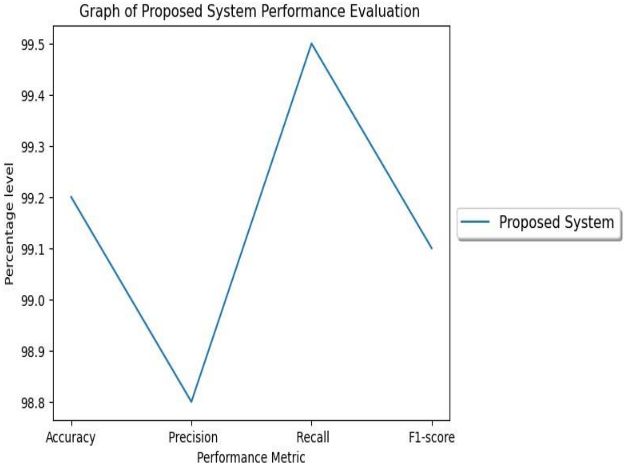


Figure 8: Performance Evaluation Graph of the proposed system

In Table 5, the proposed system show good performance of 99.2%, 98.8%, 99.5%, 99.1% and 0.008% in accuracy, precision, recall, F1-Score and False alarm reduction respectively. The system can detect MitM, DDoS, Ransomware attacks. In Figure 8, the Performance Evaluation Graph of the proposed system shows high performance.

6. CONCLUSION

This study work mutual the accuracy of fuzzy logic system for Identification and classification of different category of attack and utilized FeedForward neural network method to train and test the system, and also the system reduces the false alarm rate in IoT healthcare Wearable devices. Outcomes gotten from the proposed model are 99.2, 98.8, 99.5, 99.1 & 0.008 for accuracy, precision, recall, F1-Score and False alarm respectively. The result demonstrates that the hybrid intrusion detection system can categorize high dimensional data set with high accuracy and significantly, showing the different attacks, the occurrences include Man in the middle, DDoS and Ransomware.

7.0 REFERENCES

1. K. Mittal, and P. Batra. **Hybrid Machine Learning based Intrusion Detection System for IoT**, *International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, Greater Noida, India, 2022, pp. 65-69.
2. A. Chakraborty, S. Adhikary, A. Ghosh, P. Paul. ***Application of Machine Intelligence in IoT-Enabled Healthcare Monitoring Systems: A Case Study-Based Approach***, In Smart and Secure Internet of Healthcare Things, 1st Edition, ImprintCRC Press, 2022.
3. D. Konstantinidis, P. Iliakis, F. Tatakis, K. Thomopoulos, K. Dimitriadis, D. Tousoulis, and K. Tsioufis. **Wearable blood pressure measurement devices and new approaches in hypertension management: the digital era**, *Journal of Human Hypertension*, Vol. 36, pp. 945–951, 2022.
4. Y. Mohammed, A. S. Mohammed, H. T. Abdulkarim, C. Danladi, A. Victor, R. Edoka. **Development and Implementation of an Internet of Things (IOT) Based Remote Patient Monitoring System**, *15th International Conference on Electronics Computer and Computation (ICECCO 2019)*, IEEE, 2019, pp. 1-6.
5. M. Stuart. ***IoT Security Challenges and Mitigations: An Introduction***. Boston, MA, USA.: Rapid 7 LLC, 2016.
6. R. Jain, G. Dhand, H. Bansal, S. Shiksha, S. Sonepat, and P. Jain. **Detection Mechanism in IoT framework using Artifcial Neural Networks**, *Research Square*, 2023.
7. P. Bischoff. **Since 2016, ransomware attacks on healthcare organizations have cost the US economy $77.5bn in downtime alone**, Comparitech Limited, https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals- data/, 2023, October 23.
8. R. Sobers. **161 Cybersecurity Statistics and Trends**, Varonis, Https://www.varonis.com/blog/cybersecurity-statistics, 2024, January 4.
9. A. H. Seh, Z. Mohammad, A. Mamdouh, K. S. Amal, A. Alka, K. Rajeev, and A. K. Raees. **Healthcare Data Breaches: Insights and Implications**, *Healthcare*, vol. 8, no. 2, pp. 133, 2020.
10. A. I. Newaz, A. K. Sikder, L. Babun, and A. S. Uluagac. **HEKA: A Novel Intrusion Detection System for Attacks to Personal Medical Devices**, *IEEE Conference on Communications and Network Security (CNS)*, 2020, pp. 1-9.
11. I. Idriss, A. Mostafa, and M. Omar. **IoT security with Deep Learning-based Intrusion Detection Systems: A systematic literature review**. *IEEE Xplore*, IEEE, 2020.
12. T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. Bahaj. **Anomalybased intrusion detection system for IoT networks through deep learning model**, *Computers and Electrical Engineering*, vol. 99, 2022.
13. J. Muhamed, and M. Ajeesha. **Fuzzy Logic for Intrusion Detection System**, *Journal of Emerging Technologies and Innovative Research (JETIR)*, vol. 7, no. 12, 2020.
14. V. Abhishek, and R. Virender. **Machine Learning Based Intrusion Detection Systems for IoT Applications, Wireless Personal Communications**, *Springer Nature.*, vol. 2, no.1, pp. 123-143, 2019.
15. H. Kukreja, N. Bharath, C. Siddesh, and S. Kuldeep. **An Introduction to Artificial Neural Network**, *International Journal Of Advance Research And Innovative Ideas In Education,* vol.1, no. 5, 2016.
16. R. Yamashita, M. Nishio, K. G. Richard, and K. Togashi. **Convolutional neural networks: an overview and application in radiology**, *Insights Imaging, Springer,* vol. 9, pp. 611–629, 2018.
17. S. Waris, and Z. Ahmad. **Application of Fuzzy Logic in Academic Setup**, *Proc. 8th International Conference on Recent Advances in Statistics,* Lahore, Pakistan, 2011, pp. 367-376.

18. A. Sahoo, G. Sahoo, and U. Sahoo. **Application of Fuzzy Logic in Transport Planning,** *International Journal on Soft Computing (IJSC)*, vol. 3, no. 2, 2012.
19. N. Amelia, A. G. Abdullah, and Y. Mulyadi. **Meta-analysis of Student Performance Assessment Using Fuzzy Logic**, *Indonesian Journal of Science and Technology*, vol.4, no.1, pp. 74-88, 2019.
20. W. Zeng, and J. Li. **Fuzzy Logic and Its Application in Football Team Ranking,** *Research Article*, *The Scientific World Journal*, Hindawi Publishing Corporation, 2014.
21. D. Oladimeji. **An Intrusion Detection System For Internet Of Medical Things**, Dalhousie University, Department of Computer Science, Halifax, Nova Scotia, 2021.
22. K. Padia. ***The Role Of The Internet Of Medical Things In Healthcare.*** Retrieved from Health Works Collective : https://www.healthworkscollective.com/the-role-of-the-internet-of-medical-things-in-healthcare/, 2021.
23. B. Marr. ***Why the internet of medical things (iomt) will start to Transform Healthcare In 2018,*** Retrieved from Forbes: https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018/?sh=1b0e214e4a3c, 2018.
24. N. Suranthaa, P. Atmajab, David., M. Wicaksono. **A Review of Wearable Internet- of-Things Device for Healthcare, Procedia Computer Science**, *5th International Conference on Computer Science and Computational Intelligence,* 2021, vol. 179, pp. 936–943.
25. N. Hashim, N. Norddin, F. Idris, S. M. Yusoff, M. Zahari. **IoT blood pressure monitoring system,** *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 19, no. 3, pp. 1384-1390, 2020.
26. M. S. Norsuriati, N. M. Sobri, H. Z. Hafiszah, A. M. Nazib, W. Z. Suhaimizan, V. Ashok, and A. Mahadi. **Development of IoT Based Cuffless Blood Pressure Measurement System**, *Journal of Physics: Conference Series, International Conference on Biomedical Engineering (ICoBE)*, 2021, vol. 2071, pp. 1-7.
27. K. Albulayhi, A. A. Smadi, F. T. Sheldon, and R. K. Abercrombie. **IoT Intrusion Detection Taxonomy, Reference Architecture, and Analyses**, *Sensors*, vol. 21, no. 1, pp. 1-30, 2021.
28. H. Lin, Q. Xue, J. Feng, and D. Bai. **Internet of things intrusion detection model and algorithm based on cloud computing and multi-feature extraction extreme learning machine,** *Digital Communications and Networks*, vol. 9, pp. 111–124, 2023.
29. P. Satam. **A Methodology to Design Intrusion Detection Systems (Ids) for Iot/Networking Protocol**, A Dissertation Submitted to the Department Of Electrical and Computer Engineering, In Partial Fulfillment of the Requirements for the Degree of Doctor Of Philosophy, In the Graduate College, University of Arizona, 2019.
30. H. Lin, H. Huang, M. Lee, and J. Li. **Intrusion Detection in IoT Network Traffic Using Markov Model**, *Sensors and Materials*, vol. 36, no. 3, 1127–1134, 2024.
31. G. Thamilarasu, A. Odesile, and A. Hoang. **An Intrusion Detection System for Internet of Medical Things,** *IEEE Access*, vol. 8, pp. 181560 – 181576, 2020.
32. H. Alshahrani, A. Khan, M. Rizwan, M. S. A. Reshan, A. Sulaiman, and A. Shaikh. **Intrusion Detection Framework for Industrial Internet of Things Using Software Defined Network**, *Sustainability*, vol. 15, no. 9001, pp. 1-18, 2023.
33. E. Gyamfi, and A. Jurcut. **Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets,** *Sensors*, vol. 22, pp. 3744, 1-33, 2022.
34. S. C. Arul, A. Vijayalakshmi, and E. Abishek. **Detection of various attacks using B-GNB in health care IoT,** *Cardiometry*, pp. 787-796, 2023.
35. A. Basharat, M. M. Khan, and A. Khan. **Machine Learning Techniques for Intrusion Detection in Smart Healthcare Systems: A Comparative Analysis**, *Paper presented in 2022 4th International Conference on Smart Sensors and Application (ICSSA)*, 2022, pp. 29-33. doi: 10.1109/ICSSA54161.2022.9870973.
36. N. Sharma, and P. G. Shambharkar. **Artificial Intelligence driven Intrusion Detection Framework for the Internet of Medical Things**, *Research Square,* 2023. doi: 10.21203/rs.3.rs-2634004/v1