Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Detecting Cyber-attacks in Fog-cloud Architecture-driven IoMT Networks Using Hybrid Deep Learning Techniques

Mohita Narang[1], Nirmal Punetha[1], Aman Jatain[2]

[1]Amity University, Gurgaon
[2]K.R Mangalam University, Gurgaon

The Internet of Medical Things (IoMT) is an emerging field where the Internet of Things technology is applied to medical devices. Cyberattacks are a concern which happens on medical devices or in the network. This paper proposes a new method to detect cyberattacks in the IoMT system using a mix of Fog-cloud setup and hybrid deep learning methods. This research uses CNN and LSTM algorithms for cyberattack detection in IoMT. Also, it uses a mix of the PSO (Particle swarm Optimisation) and SCA (Sine Cosine Algorithm) optimisers. Various data preprocessing, Cross validation, Feature extraction techniques like Variance Threshold and Pearson Correlation Coefficient and hyperparameter tuning techniques are applied. So the proposed model is well-optimized for generalization and scales well. The proposed model performs well on big data and is evaluated in term of accuracy, recall, precision, and F1-score. This research presented an accuracy of 96%. Big data is handled using Spark technology. The proposed model performance is compared with various machine learning models like Random Forest, Cat-Boost, Decision Tree, Naïve Byes. This research has outperformed other existing detection methods as it gives good accuracy on a large volume of data.
Keywords: CNN, LSTM, IoMT, intrusion detection, Deep Learning.

1. Introduction

IoMT is the latest IoT field enhancement and a subset of IoT. IoMT means integrating healthcare-based devices and sensors with IoT [1]. IoMT includes numerous clinical gadgets, such as smart blood pressure monitors, smart glucometers, smart bands, smart pacers, and pulse rate monitors [2]. These healthcare devices and systems analyse and transmit health data remotely, making remote patient monitoring and diagnosis possible [3]. IoMT-enabled gadgets

have made tracking feasible inside the healthcare sector. It allows the potential to maintain patient safety and inspire physicians to offer timely treatment [9].

However, the concern is providing security to IoMT systems. This era inspires hackers to hack saved medical records. Numerous varieties of attacks would be used to control those smart medical gadgets.

Contributions of our research

1. The numerous devices and sensors that make up the IoMT environment generate enormous amounts of data. This research utilised hybrid deep learning techniques with PSO and SCA optimizers to examine massive amounts of data in real time.

2. To handle security concerns near the network's edge, fog computing, in conjunction with cloud architecture, is utilised to decentralise the stand-alone cloud-based security mechanism. This architecture improves security levels of IoMT networks by better positioning the security responses in the system as well as addressing the weaknesses of employing a central approach to security control.

3. The KDD CUP99 or NSL-KDD datasets are mainly used to evaluate most current detection systems. These datasets are out of date. Some researchers have used the ToN-IoT dataset, which contains data only for IoT/IIoT and no medical data. In our study, we addressed this gap by combining two datasets—one containing medical data and the other IoT data—integrating 14 types of cyberattacks. This realistic, multi-domain dataset allowed us to assess the effectiveness of the suggested model in terms of accuracy, precision, detection rate, false alarm rate, and F1 score. In addition, it is compared to the existing detection models [5].

2. Cybersecurity in IoMT

As the Internet of Medical Things (IoMT) expands quickly, several cyberattacks have revealed important weaknesses in the IoMT ecosystem [4]. Industry insiders have noted that many IoMT devices are susceptible to cyberattacks that could endanger patients' lives. IoMT devices use open wireless communication channels. Furthermore, the healthcare industry has developed a networked, virtualised clinical equipment ecosystem that constantly transmits unstructured, possibly unprotected, and cyberattack-prone data [19]. This network's inadequate authentication procedures and bad design make it susceptible to cyberattacks. The inability to recognise and prevent such attacks poses an additional security risk of gaining illegal access without being noticed. Consequently, an attacker might alter the medicine dosage [7].

Another challenge is that medical devices have longer lifespans than consumer goods. This means that security protocols developed during manufacturing could become outdated over time. So, a continuous update and patching process must be followed [5].

Many types of IoMT devices exist, from wearables to mobile health apps. Each has a different operating system, making the development of a universal security protocol that can protect all IoMT devices challenging [6].

Healthcare providers and device manufacturers must develop a secure IoMT ecosystem [8].

Manufacturers should develop an updated system. Healthcare providers should also ensure IoMT devices remain up-to-date with the latest software versions and security patches [7]. Another best practice is to have an access control mechanism in IoMT devices where access to IoMT devices should be limited to authorised personnel only. The access should be granted based on user roles. It can save patient data somewhat [11].

New Intrusion Detection Techniques for IoMT Cyberattacks

a. Fuzzy-based self-tuning LSTM

This method dynamically adjusts learning parameters based on data, improving accuracy and reducing false positives (An Adaptive Intrusion Detection System in the Internet of Medical Things Using Fuzzy-Based Learning). This technique increases accuracy and reduces false positive rates [9]. To handle uncertainties and ambiguities inherent in real-world data, Fuzzy logic incorporates human-like reasoning with degrees of truth (e.g., "somewhat high," "very low") where previous data was represented only by 0(False) and 1(True).

b. Ensemble learning

Combining multiple machine learning algorithms enhances detection capabilities and mitigates this risk by providing a more resilient defense against various attack types and enhancing detection capabilities [10]. For example, an ensemble system might use a decision tree to identify unusual data flow patterns. A support vector machine is trained on known attack signatures to confirm the anomaly. This combination approach reduces the false positives.

c. Federated learning

The training data is not sent to the central server but is kept on local devices. Only the model updates are sent to the server. This is done to average and redistribute the data to the participants. Blockchain is used to ensure the integrity and security of these exchanges [12].

Other Techniques

a. Anomaly detection based on context-aware behaviour

Analyzes historical and real-time data to identify deviations from normal device behaviour patterns (Towards Context-Aware Behavior-Based Intrusion Detection for the Internet of Medical Things [13]. It analyses historical and real-time data, including:

- User behaviour (e.g., login times, access patterns)

- Device activity patterns (e.g., power consumption, data transfer.

- Environmental factors (e.g., temperature, location)

b. Graph-based anomaly detection

Utilizes network topology information to detect suspicious connections and data flows [15]. It analyses the network topology, looking for:

- Unusual connections between devices.

- Sudden changes in data flow patterns.

- Deviations from expected communication patterns.

Graphs provide an additional layer of security, as they can identify lateral movements within networks that other methods might miss.

c. Blockchain-based intrusion detection

Leverages blockchain's immutability and transparency for secure intrusion detection record-keeping and decentralised decision-making (Security and Privacy Challenges in Blockchain-Based Intrusion Detection Systems for the Internet of Things [14].

3. Literature Review

A study proposed a model that uses Gray Wolf optimisation combined with Principal Component Analysis (PCA) for feature extraction. PCA was implemented after the Grey-Wolf optimiser. The Grey Wolf Optimizer overcomes the smallest local problems and achieves faster convergence than existing optimisers. However, the NSL-KDD dataset was used to evaluate the proposed model [29].

To provide post-quantum security, privacy-preserving multi-factor authentication scheme was proposed to enhance the security of cloud-enabled IoMT. Hash operations and error reconciliation technology provided highly secure and flexible authentication suitable for the cloud environment [3]. The scheme's Real-Or-Random (ROR) model was used for this. The proposed scheme was compared with state-of-the-art methods to showcase a well-balanced trade-off between security and overhead.

[34] proposed a Fed-Inforce-Fusion, a privacy-preserving Federated Learning (FL) in the Internet of Medical Things (IoMT) networks. It is based on the Intrusion Detection System (IDS) model. Reinforcement learning is combined to understand the underlying relationships in medical data and FL to train an IDS model collaboratively across distributed Smart Healthcare System (SHS) nodes while preserving privacy[17]. Fed-Inforce-Fusion employs a fusion/aggregation strategy to enhance detection performance and reduce communication overhead by allowing the dynamic participation of clients in the federation process.

Another study designed and developed a novel mobile agent-based intrusion detection system to secure the network of connected medical devices [25]. This hierarchical, autonomous system employs machine learning and regression algorithms to detect network-level intrusions and sensor data anomalies. Hospital network topology was simulated, and detailed experiments were performed on various Internet subsets of Medical Things, including connected medical devices and wireless body area networks. [19] proposed a robust cryptosystem for encrypting medical images in secure Internet of Medical Things (IoMT) and cloud services. The encryption method uses a 3D chaotic map to implement nonlinear ciphering processes for pixel value diffusion and position permutation. Five operations are performed on the medical images: 3D chaos generation, chaos histogram equalisation, row rotation, column rotation, and XOR operation, ensuring high security [39].

The suggested cryptosystem is validated using various medical images, demonstrating high-

security performance through different assessment parameters. Simulation results indicate the proposed cryptosystem's trustworthiness, robustness, and recommended security levels for healthcare, IoMT, and cloud service applications [41].

Key findings include an average entropy value of 7.95 (close to the maximum value of 8) and an average NPCR value of 99.62% (close to the maximum value of 99.60%). Comparative analysis shows the superior performance of the proposed cryptosystem over traditional security systems across various evaluation parameters. [38] implemented Principal component analysis (PCA) for feature reduction and ensemble-based classifiers to predict network intrusion attacks. And achieved 93.2 % accuracy using bagged decision trees of the bagging algorithm. KDDCup- '99' dataset has been employed, and performance is evaluated in accuracy, precision, recall, and F-score. [45] proposed an ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks is proposed. A ToN-IoT dataset is used. StackingCVClassifier is used to design ensemble learning.

4. Research Gaps

Various research gaps have been identified based on reviews of cyber-attack prevention techniques. While doing the literature review, we found the following research gaps:

- It was identified that researchers have mainly used data sets like NSL-KDD and KDD CUP 99. These datasets are obsolete datasets lacking IoMT attacks and do not contain medical data. So, we used publicly available dataset (WUST EHMS 2020 and EDGE-IIOTSET), which was recently published and have medical data.

- Intensive research has not been found to detect cyberattacks like spoofing and data injection attacks, so our research will be focused on them.

- This research used the latest IoMT and IIoT datasets containing 14 + attacks and Spark technology to handle big data—detection and defence form of various cyber-attacks, such as spoofing, man-in-the-middle attacks, and data injection. It was identified that most of the research are not handling big data.

- Limited research has been conducted on fog-cloud architecture, leaving significant potential for further exploration.

5. CNNLSTM-PSO+SCA

Long-short-term memory (LSTM) networks are a type of recurrent neural network (RNN) capable of learning long-term dependencies in data. They are beneficial for processing sequential data, such as time series, natural language, and audio signals [16].

Convolutional Neural Networks (CNNs) are a type of neural network that is particularly effective at learning hierarchical patterns in data [18]. They are commonly used for image and video recognition tasks but can also be applied to other data types, such as audio and text.

CNNLSTM networks combine the strengths of LSTMs and CNNs by using CNNs to extract features from sequential data, which are then passed through an LSTM network for further

processing [20]. It allows the network to learn the data's short-term and long-term dependencies and hierarchical patterns.

Through the effective tuning of the hyperparameters and model weights of the CNN-LSTM architecture, PSO and SCA in combination effectively improves the cyberattack detection in IoMT scenarios. While PSO guarantees the global optimization making sure there are no local minima, SCA aids in enhancing the exploration and exploitation of the search space. Because of this, the CNN-LSTM model is able to capture the spatial and temporal dimensions of the IoMT data processed with greater precision even when the data s comprising of noise, class imbalance and dealing with complicated attacks.

6. Model Architecture

This research used Fog layer where data processing and detection is happening. After that the data is sent to cloud. Fog layer is able to simplify the processing of data at the edge of the network by deploying local nodes that execute real-time analysis near the location of devices in IoMT. Fog nodes are deployed near IoMT devices in order to carry out data processing for immediate threat detection. In order to protect sensitive data, local data processing at the fog nodes reduces the risk of transmission [40].

Lessens the burden of moving large volumes of data often to the cloud, allowing for real-time intrusion detection—essential in critical healthcare applications. Fog nodes identify and learn the local behavior patterns and improves anomaly detection.

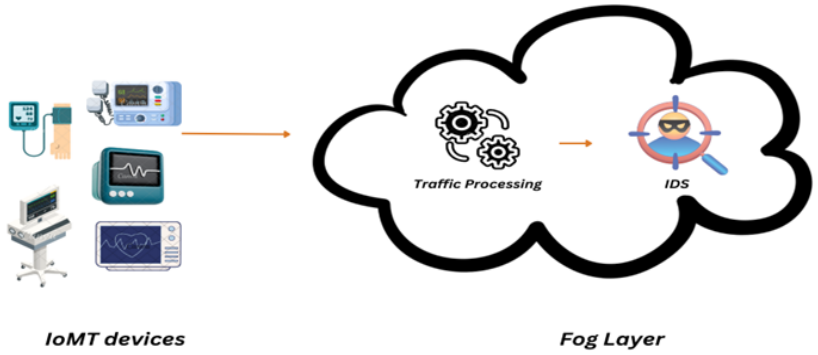

Figure 1. Model Architecture

- Data from different medical devices is retrieved to check if it is malicious, as shown in Fig. 1.

- Sensors on the IoMT network include a temperature sensor, blood oxygen saturation (SpO2) sensor, an electrocardiogram (ECG or EKG) sensor, and a blood pressure sensor [23].

- The medical sensors are connected to the multi-sensor board via each wire connector and to the patient’s body [26].

- These sensor nodes monitor and collect data and forward it to the local gateway node via the multi-sensor board, which connects to a Windows-based computer via a USB port [25].

- Then, the collected data is sent to the fog layer, as shown in Fig 1.

- Before sending the data to the fog layer, we will have switches, routers, and gateways to help quantify the traffic flow and minimise network traffic overhead [27].

- IoMT traffic is sent to the predictive model to distinguish the attack from regular instances. Traffic will pass through the following components:

Traffic processing

Data preprocessing involves checking for missing values, selecting features, normalising data, and handling it.

a. Handling Missing Values

There are many missing values in the dataset which needs to be handled. We handled it using Imputation.

1. Imputation

• Mean Imputation: Missing values are substituted with the mean of the feature.

• Median Imputation: Missing values are replaced by the median value of the feature.

2. Data Removal

Columns or rows which possess a significant amount of missing data are eliminated. This is done if they exceed the certain threshold set by the user.

b. Feature Selection

Selecting the features which are most relevant to the task has some benefits such as improving accuracy, avoiding overfitting and increasing interpretability. The techniques that belong to this category rank the significance of features that have relevance to others in the model.

• Variance Threshold

Low-variance features provide less information and scope and can be ignored or removed from the data set. They way a threshold is defined such that only those features are retained that have some variation that is significant.

• Correlation Analysis

Highly correlated features contribute to redundancy, for one of them can be deleted. This also reduces the risk of multicollinearity and boosts model performance.

3. Data Normalization

Normalization makes sure that each and every model feature is on the same scale which helps in training the model efficiently. Min-Max Scaling and Standardization are the techniques that are commonly employed. Min-Max Scaling technique adjusts each feature into a range that has boundaries set

Intrusion detection system

The detection of malicious activities in the incoming data is done. Once done, it is forwarded

to the cloud layer for storage. The Cloud layer will also have a traffic processing and intrusion detection module for traffic preprocessing and intrusion detection [24]. Deep learning methods, such as Convolutional Neural Network - Long Short-Term Memory (CNNLSTM) are being used to refine the feature selection process and detect intrusions in cloud environments. These approaches have been shown to improve accuracy and reduce false positives significantly.

However, if there is malicious activity in the traffic, the administrator will be notified, and appropriate measures will be taken to prevent the intrusion. Otherwise, the data is stored in the cloud [34]. However, the efficiency of the proposed model is evaluated in terms of accuracy, detection rate, false-positive rate, and F1 score [28].

7. About Dataset

Two datasets were used in this research. Dataset1 is the IoMT malware dataset named WUSTL EHMS 2020 dataset for the Internet of Medical Things (IoMT) Cybersecurity) with 16,000 records that contain features such as heart rate, max and min packet sizes, temperature, number of source and destination bytes, source port, source and destination load, pulse rate, destination port, jitter, temperature, respiratory rate, Spo2, diastolic and systolic pressure and a label which indicates whether the dataset is malware (1,0). Another is the Edge-IIoTset Cyber Security Dataset. Data is collected from various IoT devices like Low-cost digital sensors for sensing temperature and humidity, Ultrasonic sensor, Water level detection sensor, pH Sensor Meter, Soil Moisture sensor, Heart Rate Sensor, Flame Sensor, ...etc. [31]. Fourteen IoT and IIoT connectivity Protocol attacks are categorised into five threats: DoS/DDoS attacks, Information gathering, Man-in-the-Middle attacks, Injection attacks, and Malware attacks. We combined these two datasets, resulting in 2235519 rows and 107 parameters.

8. Experimental Results

Before model implementation, we used Normalization and Standardization to transform and scale the data. We followed the traditional IDS approach for test pre-processing, such as KFold, NaN Founder, etc. Techniques like the Correlation Matrix, Variance Threshold, and Fisher Score are used for feature selection.

As discussed, we used two datasets. Dataset 1 has multiple attack datasets that do not have man-in-the-middle attacks. Hence, we are merging dataset 1 with dataset 2. Dataset 2 has data related to man-in-the-middle attacks. The data size after merging both datasets is (2235519, 107). Then, the data size is calculated after merging both datasets. Our dataset is converted to a big dataset that can be accessed by Spark technology. The dataset is normalised using IP-based attributes.

Feature Extraction

While dealing with high dimensional data, Feature extraction is an important step in machine learning flow. In this important feature are only selected. It reduces computational cost, and enhance interpretability.

a. Variance Threshold

Variance Thresholding is a simple technique in which features with low variance are removed. These low variance features are typically constant or nearly constant throughout the dataset. So, they provide little information for predictive modeling tasks. So, eliminate these low-variance features. This reduces noise in the data and improve model performance. Variance Threshold removes features whose variance doesn't meet a threshold. By default, it removes all zero-variance features, i.e., features with the same value in all samples [30].

```
58
icmp.checksum
icmp.seq_le
http.content_length
http.response
udp.stream
udp.time_delta
dns.qry.name
dns.qry.qu
dns.retransmission
dns.retransmit_request
dns.retransmit_request_in
mbtcp.len
mbtcp.trans_id
mbtcp.unit_id
Attack_label
SrcAddr
DstAddr
Dport
SrcBytes
DstBytes
SrcLoad
```

Figure. 2. Important features

There are 89 columns in total. Of these, 58 are considered important, as shown in Fig. 2. above, and the remaining are considered unwanted.

b. Pearson Correlation Coefficient

Pearson's correlation coefficient is the test statistic that measures the association, or statistical relationship, between two continuous variables [33].

In disciplines like statistics, physics, and the social sciences, Pearson's correlation coefficient is one of the most often utilised statistics for determining the connection between variables [16].

This technique analyses the correlation between the columns. The columns that are not related to any other column are removed. The number of correlation features is 13. They are dropped [32].

During mutual information classification, data is classified as continuous or binary. Continuous indicates the sequence of numbers in each column. That should be removed. Binary should be retained [35].

```
{'arp.hw.size',
 'mqtt.conack.flags-0x00000000',
 'mqtt.conflags',
 'mqtt.len',
 'mqtt.msgtype',
 'mqtt.proto_len',
 'mqtt.protoname-0',
 'mqtt.protoname-MQTT',
 'mqtt.topic-0',
 'mqtt.topic-Temperature_and_Humidity',
 'mqtt.topic_len',
 'mqtt.ver',
 'tcp.flags.ack'}
```

Figure. 3 Correlated Features

MinMaxScaler scales all the data features in the range [0, 1] or else in the range [-1, 1] if the dataset has negative values [40]. In other words, it scales the minimum and maximum values to be 0 and 1, respectively [37].

After standardisation, the test train of X and Y is indicated.

9. Proposed CNN-LSTM

CNN-LSTM Model, a combination of CNN and LSTM Neural Network, for training. This model is proposed in this research.

A hybrid novel approach to optimisation combining PSO (Particle swarm Optimisation) and SCA (Sine Cosine Algorithm), which belong to different categories of optimisation techniques.

PSO is inspired by the collective behavior of decentralized, self-organized systems. The individual particles communicate and cooperate to find the best solution. PSO+SCA optimisation will calculate the optimum points and provide the optimum point for the entire dataset. The common optimum point will help us select our training feature. It helps the model to get trained properly, significantly improving the traditional CNLSTM model [36].

Hyperparameter tuning uses cross-validation using the k-fold method. It is performed using grid search cross-validation, batch size, and epochs using 5 split K-fold. Some parameters are added [38].

```
Model: "sequential_1"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 conv1d_2 (Conv1D)           (None, 14, 128)           1024

 max_pooling1d_2 (MaxPooling  (None, 7, 128)           0
 1D)

 conv1d_3 (Conv1D)           (None, 7, 64)             57408

 max_pooling1d_3 (MaxPooling  (None, 3, 64)            0
 1D)

 bidirectional_3 (Bidirectio  (None, 3, 1024)          2363392
 nal)

 batch_normalization_3 (Batc  (None, 3, 1024)          4096
 hNormalization)


 bidirectional_4 (Bidirectio  (None, 3, 512)           2623488
 nal)

 batch_normalization_4 (Batc  (None, 3, 512)           2048
 hNormalization)

 bidirectional_5 (Bidirectio  (None, 256)              656384
 nal)

 batch_normalization_5 (Batc  (None, 256)              1024
 hNormalization)

 dense_1 (Dense)             (None, 2)                 514

=================================================================
Total params: 5,709,378
Trainable params: 5,705,794
Non-trainable params: 3,584
_________________________________________________________________
```

Figure. 4. Model Summary

While training the CNNLSTM model, we observed that loss and root mean square error decreased with every epoch. It shows that the model is functioning properly [43]. This was done by implementing early stopping and hyperparameter tuning. Early stopping prevents overfitting by halting the training once the loss or RMSE increases on the validation set. GridsearchCV was implemented for hyperparameter tuning [38].

Optimisation Using PSO and SCA

SCA optimises data further using ABC. Below Fig. 5. represents the metrics score for CNN+LSTM with PSO and SCA.

```
Accuracy: 95.90%
Recall: 95.90%
Precision: 96.54%
F1-Score: 95.81%
```

Figure 5. Metrics score for CNNLSTM+ABC+SCA+PSO

When CNNLSTM was implemented with PSO+SCA optimisers then we received accuracy of around 96%, recall value 95.90%, precision of 96.54% and F1 Score of 95.81%. A recall of 95.90% means that out of all the actual positive instances, 95.90% were correctly identified by the model. A precision of 96.54% means that when the model predicts a positive case, 96.54% of the time, it is correct. F1-score of 95.81%, the model demonstrates balanced performance, excelling in both identifying true positives (recall) and avoiding false positives (precision).

Table 1. Comparison with other ML Algorithms

	Accuracy	Recall	Precision	F1-Score	time to train	time to predict
Naive Bayes	0.800	0.8000	0.8000	0.8000	0.008002	0.000000
Random Forest	0.940	0.9400	0.9400	0.9400	0.212943	0.015705
Cat-Boost	0.870	0.8700	0.8700	0.8700	4.759364	0.013975
K-Nearest Neighbors	0.800	0.8000	0.8000	0.8000	0.072998	0.086917
Decision Tree	0.909	0.9090	0.9100	0.9095	0.016072	0.000000
AdaBoost	0.880	0.8800	0.8800	0.8800	0.626998	0.015797
CNN+LSTM	0.940	0.9400	0.9400	0.9400	0.575990	0.015618
CNNLSTM+PSO+SCA	0.959	0.9591	0.9554	0.9581	1.253996	0.031594

Different machine learning algorithms like Decision Tree, Naive Bayes, Cat-Boost, AdaBoost, K-Neighbors and Random Forest are implemented, and performance is compared with the proposed model CNNLSTM and later with CNNLSTM+PSO+SCA. The proposed model gave an accuracy of 96%, whereas Naive Bayes performed poorly compared to other algorithms by giving 80% accuracy. K-Nearest Neighbors gave the same score for all the metrics as Naive Bayes. Random Forest performed equal to CNNLSTM, but its performance was not comparable to CNNLSTM+PSO+SCA in terms of all the metrics (accuracy, precision, recall, F1 score). Naïve Bayes take only 0.008 seconds for training and Cat-Boost is the slow performer in terms of training i.e. 4.75 seconds, likely due to its ensemble structure.

10. Experimental Results

The proposed model is compared with the existing study conducted in IoMT. The comparison is done in Table 2.

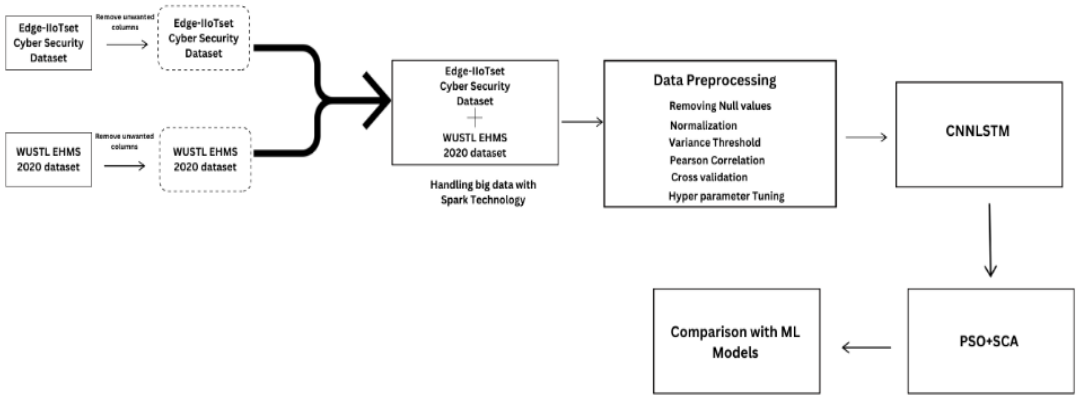

Fig 6 Framework of the proposed hybrid attack detection system

After combining both datasets data preprocessing is performed and then CNNLSTM model is applied and used PSO+SCA optmizers and the results are compared with different ML models.

Table 2. Comparison of the proposed model with the existing study

Model	Accuracy	Recall	Precision	F1 Score
Proposed SVM[24]	0.958	0.95	0.95	0.947
Fuzzy-based LSTM model[23]	0.948	-	0.15	0.952
Swarm-neural net-work-based model	0.89	-	-	-
Bagged decision trees[25]	0.932	-	-	-
CNN+LSTM	0.940	0.940	0.940	0.940
CNN+LSTM+PSO+SCA	0.959	0.959	0.958	1.253

The accuracy of the CNN-LSTM model, was 94%. This performance of CNNLSTM was enhanced by incorporating the Particle Swarm Optimisation (PSO) and the Sine Cosine Algorithm (SCA) for optimisation [35]. This optimisation technique aims to improve the accuracy and efficiency of cyberattack detection, making it a powerful tool for securing IoMT networks. So, the CNN+LSTM+PSO+SCA model was implemented to increase the accuracy [22].

CNNLSTM models provide valuable insights into effective detection and mitigation strategies for cyber threats [46]. This represents cutting-edge research in the field of cybersecurity for IoMT networks. Most of the research focused only on DDoS detection [11]. Our research is detecting different cyberattacks. The WUSTL EHMS 2020 dataset was used by Tauqeer et al., 2022, but our research can also handle big data. In [25], the KDDCup-'99' dataset is used. Models like RF, Bagged Decision Trees, Extra Trees, Logistic Regression AdaBoost, Stochastic Gradient, and SVM were compared with bagged decision trees [18].

Table 1 and figure 7 shows that CNNLSTM+PSO+SCA gives the highest accuracy, i.e. 96%, and K-nearest Neighbor and Naive Bayes have the lowest accuracy, i.e. 80%. Figure 8, 9 and figure 10 show that CNNLSTM+PSO+SCA has the Highest recall precision and F1 Score value.

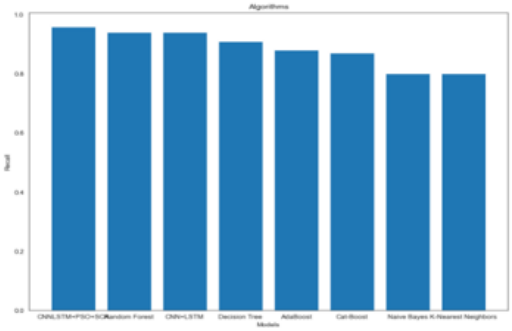

Figure 7 Accuracy

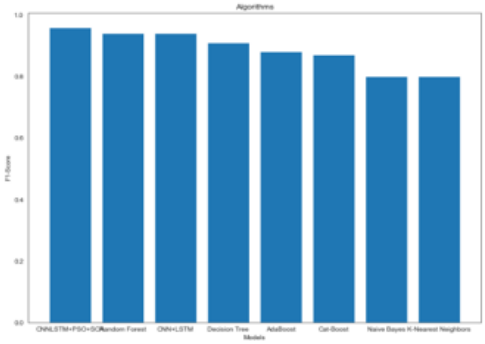

Figure 8 F1 score

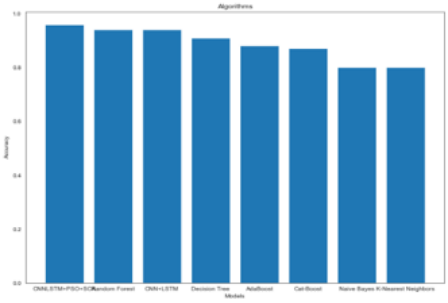

Figure 9 Recall

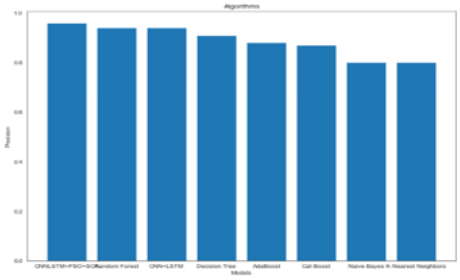

Figure 10 Precision

K-Nearest Neighbor and Naïve Bayes continuously to give the lowest recall precision and F1 Score values. It was noticed that Random Forest and CNNLSTM performed equivalently in accuracy, precision and recall. However, CNNLSTM+ABC+SCA improved the metrics' score compared to CNNLSTM and Random Forest [42].

11. Comparing Proposed Model with Existing study

SafetyMed detects malicious image data and sequential network traffic with accuracy of 97.63% using CNNLSTM. Since this research did not use hyperparameter tuning, there is a possibility that the model may be overfitted. The CIC-IDS2017 dataset used in this research is considered outdated [11]. This research used six machine learning (ML) and deep learning (DL) models and deep learning models like Convolutional Neural Network (CNN), hybrid CNN-Long Short-Term Memory (LSTM), and an attention-based hybrid CNN-LSTM. The main drawback of this research is that it used ToN_IoT which does not contain medical data. Secondly it used single dataset but out research used combination of two datasets which contains medical data. Our research employed cross-validation techniques for improving model reliability and generalization, which was not utilized in this other study [22]. Another study proposes RCLNet, an effective Anomaly-based Intrusion Detection System (A-IDS) for IoMT. This study used only one dataset which is WUST EHMS 2020 dataset. Secondly it used ADAM optimizer with CNNLSTM. Using Adam optimizer with a CNN-LSTM for IoMT

cyberattack detection can lead to sensitivity to imbalanced data, overfitting and unstable convergence due to its adaptive nature. But our research used PSO+SCA optimizers which can handle imbalanced IoMT data, and reduce overfitting [16]. A Recent study proposed the solution of detecting cyberattacks by using CNN on dataset. This study face challenges such as real-time performance, integration with existing infrastructure. This challenge can be addressed by using SDN. Our research uses PSO+SCA for automated hyperparameter optimization. So can scale well and may generalize better to new datasets but [32] used Adam optimiser relies on manual tuning, which might not be scalable or repeatable.So this research is suitable for small scale datasets and our research is suitable for real-world applications where big data is involved.

Besides handling the big data our research is capable of providing low-latency, scalable, and efficient cyberattack detection as it is using Fog Cloud architecture and the other researches have not used this. Secondly, we combined two dataset and leveraged spark technology to handle bigdata. Third we used PSO+SCA optimizers which optimizes hyperparameters and model weights effectively. [8] demonstrated how PSO-based CNN-LSTM model can outperformed a standard CNN in intrusion detection tasks. It highlights PSO's effectiveness in optimizing complex neural network.

12. Conclusion

This research work was tested using a Fog-cloud architecture, and machine learning and deep learning algorithms were implemented to detect cyberattacks in the Internet of Medical Things (IoMT) networks. A unique hybrid approach was used to detect cyber-attacks using convolutional neural networks (CNNs) and long short-term memory (LSTM) algorithms. Different machine learning algorithms like RF, Decision Tree, Naive Bayes, Cat-Boost, AdaBoost, and K-Neighbors were also used for detection experiments. A hybrid optimisation method enhanced the model's performance, including Artificial BeeColony (ABC) and Sine Cosine Algorithm (SCA). Our model achieved an accuracy of 96% and handled the big data very effectively. The proposed model can be improved by implementing the transformers-based algorithm in a real-world IoMT environment. Machine learning models' accuracy for detecting cyber-attacks in the IoMT is lower than desired. Adding more varied datasets (including recent cyberattacks) will help the model become more broadly applicable. Data augmentation approaches can be used intentionally to generate variants of already-existing data

References

1. Algarni, A. (2019). A Survey and Classification of Security and Privacy Research in Smart Healthcare Systems in IEEE Access, 7, pp. 101879-101894. https://doi.org/10.1109/ACCESS.2019.2930962
2. Lokshina, I., Lanting, C. 2019. A qualitative evaluation of IoT-driven eHealth: Knowledge management, business models and opportunities, deployment and evolution in Data-Centric Business and Applications, Springer pp. 23–52.
3. Chen, X., Wang, B., & Li, H. (2024). A privacy-preserving multi-factor authentication scheme for cloud-assisted IoMT with post-quantum security in Journal of Information Security and

Applications, 81, pp. 103708.
4. Wang, E. K., Chen, C.-M., Hassan, M. M., Almogren, A. 2020. A deep learning-based medical image segmentation technique in the internet-of-medical-things domain in Future Generation Computer Systems, 108, pp. 135–144.
5. Sikarndar, M., Anwar, W., Almogren, A., Din, I. U., Guizani, N. 2020. IoMT-based association rule mining for the prediction of human protein complexes in IEEE Access, 8, pp. 6226–6237.
6. El-Banby, G. M., Elazm, L. A. A., El-Shafai, W., et al. (2024). Security enhancement of the access control scheme in IoMT applications based on fuzzy logic processing and lightweight encryption in Complex Intelligent Systems, 10, 435–454. https://doi.org/10.1007/s40747-023-01149-6
7. Majeed, F., Nazir, M., Schneider, J. 2023. ISA: Internet of Medical Things (IoMT) in Smart Healthcare and its Applications: A Review in 3rd International Conference on Artificial Intelligence (ICAI), pp. 129-135, Islamabad, Pakistan.
8. Kim, TY., Cho, SB. (2019). Particle Swarm Optimization-Based CNN-LSTM Networks for Anomalous Query Access Control in RBAC-Administered Model. In: Pérez García, H., Sánchez González, L., Castejón Limas, M., Quintián Pardo, H., Corchado Rodríguez, E. (eds) Hybrid Artificial Intelligent Systems. HAIS 2019. Lecture Notes in Computer Science(), vol 11734. Springer, Cham. https://doi.org/10.1007/978-3-030-29859-3_11
9. F. 2020. Internet of things: A survey on machine learning-based intrusion detection approaches in Computer Networks, 151, pp. 147–157.
10. Hatzivasilis, G., Soultatos, O., Ioannidis, S., Verikoukis, C., Demetriou, G., Tsatsoulis, C. 2019. Review of security and privacy for the Internet of Medical Things (IoMT) in 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), pp. 457–464, IEEE.
11. Faruqui, Nuruzzaman, Mohammad Abu Yousuf, Md Whaiduzzaman, AKM Azad, Salem A. Alyami, Pietro Liò, Muhammad Ashad Kabir, and Mohammad Ali Moni. 2023. "SafetyMed: A Novel IoMT Intrusion Detection System Using CNN-LSTM Hybridization" Electronics 12, no. 17: 3541. https://doi.org/10.3390/electronics12173541
12. Priyadarshini, R., Panda, M. R., Mishra, B. K. 2019. Security in healthcare applications based on fog and cloud computing. Cyber Security. Parallel Distributed Computing., pp. 231-243.
13. Yaacoub, J.-P. A., Noura, M., Noura, H. N., Salman, O., Yaacoub, E., Couturier, R., Chehab, A. 2020. Securing internet of medical things systems: Limitations, issues and recommendations in Future Gener. Comput. Syst., 105, 581-606.
14. Karageorgou, M., et al. 2020, Cybersecurity attacks on medical IoT devices for smart city healthcare services. In F. AI-Turjman & M. Imran (Eds.), Institution of Engineering & Technology (pp. 171-187). https://doi.org/10.1049/PBCE128E_ch8
15. Lu, Y., Qi, Y., & Fu, X 2019, A framework for intelligent analysis of digital cardiotocographic signals from IoMT-based foetal monitoring. Future Generation Computer Systems, 101(C), 1130-1141. https://doi.org/10.1016/j.future.2019.07.052
16. Shaikh JA, Wang C, Muhammad WUS, Arshad M, Owais M, Alnashwan RO, Chelloug SA, Muthanna MSA, 2024 Oct, RCLNet: an effective anomaly-based intrusion detection for securing the IoMT system in Front Digit Health. doi: 10.3389/fdgth.2024.1467241. PMID: 39421756; PMCID: PMC11484052.
17. Al-Turjman, F., Nawaz, M. H., Ulusar, U. D. 2020. Intelligence in the Internet of Medical Things era: A systematic review of current and future trends in Comput. Commun., 150, pp. 644-660.
18. Alsubaei, F., Abuhussein, A., Shandilya, V., Shiva, S. 2019. IoMT-SAF: Internet of Medical Things security assessment framework in Internet of Things, 8, pp. 100123.
19. El-Shafai, W., Khallaf, F., El-Rabaie, E. S. M., et al. (2024). Proposed 3D chaos-based medical image cryptosystem for secure cloud-IoMT eHealth communication services. Journal of Ambient Intelligence and Humanized Computing, 15, pp. 1–28. https://doi.org/10.1007/s12652-022-03832-x
20. Alalhareth, M., Hong, S.-C. 2023. An adaptive intrusion detection system in the Internet of Medical

Things using fuzzy-based learning. Sensors, in Artificial Intelligence and Internet of Things in Healthcare Systems, 23(22),pp. 9247.

21. Zhang, H., Li, G., Zhang, Y., Gai, K., Qiu, M. August 14–16, 2021. Blockchain-based privacy-preserving medical data sharing scheme using federated learning in Knowledge Science, Engineering and Management, 14th International Conference, KSEM 2021, Tokyo, Japan.
22. Zachos, Georgios, Ismael Essop, Georgios Mantas, Kyriakos Porfyrakis, José C. Ribeiro, and Jonathan Rodriguez. 2021. An Anomaly-Based Intrusion Detection System for Internet of Medical Things Networks in Electronics 10, no. 21: 2562. https://doi.org/10.3390/electronics10212562
23. Pacheco, J., Benitez, V. H., Félix-Herrán, L. C., Satam, P. 2020. Artificial Neural Networks-Based Intrusion Detection System for Internet of Things Fog Nodes in IEEE Access, 8, pp. 73907-73918.
24. Alzuabi, W., Ismail, Y., Elmedany, W. 2022. Privacy and Security Issues in Blockchain-based IoT Systems: Challenges and Opportunities in International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), pp. 258-265.
25. Thamilarasu, G., Odesile, A., & Hoang, A. 2020. An intrusion detection system for Internet of Medical Things. IEEE Access, 8, pp. 181560-181576. https://doi.org/10.1109/ACCESS.2020.3026260.
26. Tauqeer, H., Iqbal, M., Ali, A., Zaman, S., Chaudhry, M. U. 2022. Cyberattacks Detection in IoMT using Machine Learning Techniques in Journal of Computing & Biomedical Informatics, 44. 10.56979/401/2022/80.
27. Kumar, P., Gupta, G. P., Tripathi, R. 2021. An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks in Computer Communications, 166, pp. 110-124
28. Algarni, A. 2019. A Survey and Classification of Security and Privacy Research in Smart Healthcare Systems. IEEE Access, 7, pp. 101879-101894.
29. Swarna Priya, R. M., Praveen Kumar Reddy Maddikunta, Parimala M., Srinivas Koppu, Thippa Reddy Gadekallu, Chiranji Lal Chowdhary, & Mamoun Alazab. (2020). An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. Computer Communications, 160, pp. 139-149.
30. Al-Abbasi, A., Karimipour, H., Dehghantanha, A., Parizi, R. M. 2020. An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System. IEEE Access, 8, pp. 83965-83973.
31. Karimipour, H., Dehghantanha, A., Parizi, R. M., Choo, K. R., Leung, H. 2019. A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids. IEEE Access, 7, pp. 80778-80788.
32. Mohamadi A, Aminian A, Ghahramani H,2024, Advanced Cyberattack Detection in Internet of Medical Things (IoMT) Using Convolutional Neural Networks in Iranian Conference on Intelligent Systems (ICIS), DOI:10.48550/arXiv.2410.23306
33. J. B., Abiodun, K. M., Adeniyi, E. A., Folorunso, S. O., Jimoh, R. G. 2022. A Deep Learning-Based Intrusion Detection Technique for a Secured IoMT System. Informatics and Intelligent Applications, Communications in International Conference on Communications, 1-6., vol 1547.
34. Khan, I. A., Razzak, I., Pi, D., Khan, N., Hussain, Y., Li, B., & Kousar, T. (2024). Fed-Inforce-Fusion: A federated reinforcement-based fusion model for security and privacy protection of IoMT networks against cyber-attacks. Information Fusion, 101, pp. 102002.
35. Tai, Y., Gao, B., Li, Q., Yu, Z., Zhu, C., Chang, V. 2021. Trustworthy and Intelligent COVID-19 Diagnostic IoMT Through XR and Deep-Learning-Based Clinic Data Access in IEEE Internet of Things Journal, 8(21), 15965-15976.
36. S. Rehman, M. Khaliq, S. I. Imtiaz, A. Rasool, M. Shafiq, A. R. Javed, Z. Jalil, and A. K. Bashir, DIDDOS: An approach for detection and identification of Distributed Denial of Service (DDoS) cyberattacks using Gated Recurrent Units (GRU) in Future Generation Computer Systems, vol.

118, pp. 453-466, May 2021. DOI: 10.1016/j.future.2021.01.022.
37. S. S. Hameed, A. Selamat, L. A. Latiff, S. A. Razak, O. Krejcar, H. Fujita, M. N. A.Sharif, and S. Omatu, A Hybrid Lightweight System for Early Attack Detection in the IoMT Fog, Sensors, vol. 21, no. 24, pp. 8289, DOI: 10.3390/s21248289.
38. T. Saba, Intrusion Detection in Smart City Hospitals using Ensemble Classifiers, in Proceedings of 2020 13th International Conference on Developments in eSystems Engineering (DeSE), Liverpool: UK, pp. 418-422, 2020. DOI: 10.1109/DeSE51703.2020.9450247.
39. M. A. Ferrag, L. Shu, H. Djallel, and K.-K. R. Choo, Deep Learning-Based Intrusion Detection for Distributed Denial of Service Attack in Agriculture 4.0 in Electronics, vol. 10, no. 11, pp. 1257, May 2021. DOI: 10.3390/electronics10111257.
40. Y. Li, Y. Zuo, H. Song, Z. Lv, Deep Learning in Security of Internet of Things in IEEE Internet of Things Journal, vol. 9, no. 22, pp. 22133-22146, Nov. 2022. DOI: 10.1109/JIOT.2021.3106898.
41. A. M. Kumaar, D. Samiayya, P. M. D. R. Vincent, K. Srinivasan, C. Y. Chang, and H. Ganesh, A Hybrid Framework for Intrusion Detection in Healthcare Systems Using Deep Learning in Frontiers in Public Health, vol. 9, pp. 1-18, Jan. 2022. DOI: 10.3389/fpubh.2021.824898.
42. F. Ullah, H. Naeem, S. Jabbar, S. Khalid, M. A. Latif, F. Al-turjman, and L. Mostarda "Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach," IEEE Access, vol. 7, pp. 124379-124389, Aug. 2019. DOI: 10.1109/ACCESS.2019.2937347.
43. P. Kumar, G. P. Gupta, and R. Tripathi, Toward Design of an Intelligent Cyber Attack Detection System using Hybrid Feature Reduced Approach for IoT Networks in Arab Journal of Science and Engineering, vol. 46, pp. 3749-3778, Jan. 2021. DOI: 10.1007/s13369-020-05181-3.