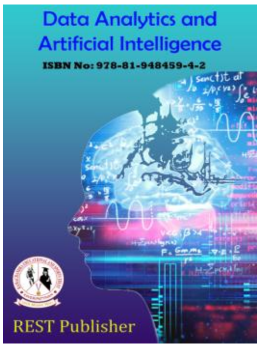
Data Analytics and Artificial Intelligence

Vol: 3(2), 2023

REST Publisher; ISBN: 978-81-948459-4-2

Website: http://restpublisher.com/book-series/daai/

DOI: https://doi.org/10.46632/daai/3/2/19


Data Analytics and Artificial Intelligence
ISBN No: 978-81-948459-4-2
REST Publisher

Malware detection in IOMT (MDI) using RNN-LSTM

***M. Uma Maheshwari, M. Suguna**

St. Joseph's College of Arts and Science for Women, Hosur, Tamil Nādu, India.

*Corresponding Author Email: umamahe996@gmail.com

Abstract. *The Internet of Things (IoT) has recently emerged as a cutting-edge technology for creating smart environments. The Internet of Things (IoT) connects systems, applications, data storage, and services, which may be a new entry point for cyber-attacks as they provide continuous services in the organization. At the current time, software piracy and malware attacks pose significant threats to IoT security. These threats may grab vital information, causing economic and reputational harm. The Internet of Medical Things (IoMT) is a subset of the Internet of Things in which medical equipment exchanges highly confidential with one another. These advancements allow the healthcare industry to maintain a higher level of touch and care for its patients. Security is viewed as a significant challenge in any technology's reliance on the IoT. Remote hijacking, impersonation, denial of service attacks, password guessing, and man-in-the-middle are all security concerns. Critical data associated with IoT connectivity may be revealed, altered, or even rendered inaccessible to authenticated persons in the event of such attacks. the deep recurrent neural network is used to detect malicious infections in IoT networks by displaying color images. In this paper, we propose a method for detecting cyber-attacks on IoMT systems that tends to make use of innovative deep learning. Specifically, our method incorporates a set of long short-term memory (LSTM) modules into a detector ensemble using a recurrent neural network.*

Keywords: *Internet of Things, cyber-attack, software piracy, malware detection, recurrent neural network (RNN), long short-term memory (LSTM), Decision Tree(DT).*

1. INTRODUCTION

The Internet of Things (IoT) is a network that connects physical objects such as smartphones, home appliances, vehicles, cameras, toys, medical tools, people, technological frameworks, structures, and animals to the Internet through a specific protocol and data sensing devices, enabling data sharing and exchanging information as well as intelligent identification, tracking, placement, monitoring, and administration [1]. The goal of the Internet of Things is to enable things to be connected at anytime, anywhere, with anyone and anything, preferably over any network and with any support [2]. The Internet of Things-enabled technologies can be used to create smart cities, education systems, e-commerce, and e-banking, maintain our health, manage industry, and entertain and protect humans [3]. Because IoT devices are always available on the network, they can be used for open attacks.

Challenges of IoT: Malware infection and pirated software can easily target the IoMT cloud for harmful usage and security negotiated settlement Software piracy is the illegal use of source codes from someone else's work to create software that impersonates the original version. Malware attacks are typically designed to compromise the privacy of IoT nodes, computer systems, and smartphones connected to the internet. Several scanning techniques based on particular profiles are proposed to detect Windows-based malware. The malware identification analysis is divided into two approaches: static and dynamic. The dynamic approach involves learning malware patterns while executing code in a real-time virtual environment. Malicious behavior can be detected through function calls, function parameter exploration, data flow, instruction traces, and visual code inspection [4]. There are automated online tools available for investigating the dynamic behavior of malicious code. Specifically, CW Sandbox, Anubis, and TT analyzer. This method takes more time because it monitors every dynamic behavior of the source code. Static malware analysis methods do not require program code implementation of program code in real time. It could be used to obtain information about the layout of malware binaries. Static signature-based malware identification techniques include control flow graph, op code frequency, n-gram, and string signature. The Internet of Things has numerous applications. Smart health services, smart grids, smart transportation, and smart buildings are all well-known applications

The framework of IoT: The Internet of Things (IoT) is a new paradigm in which a network of real world objects equipped with sensors aims to seamlessly integrate the digital and physical worlds [5]. The Internet of Things revolution is reimagining modern healthcare and changing its reliability and delivery, thanks in large part to advances in sensor networks, wireless communications, cloud computing, and mobile devices. Figure 1 depicts the four-layer design of the IoT

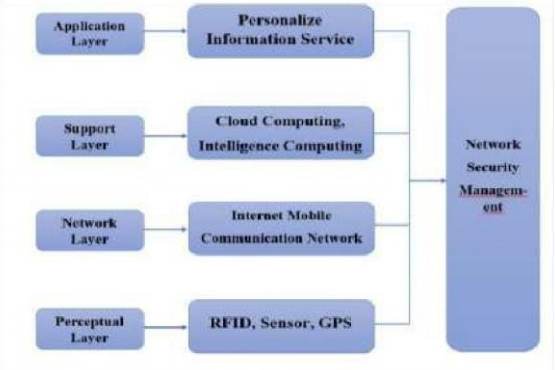

Application Layer
Personalize Information Service
Support Layer
Cloud Computing, Intelligence Computing
Network Layer
Internet Mobile Communication Network
Perceptual Layer
RFID, Sensor, GPS
Network Security Managem-ent

FIGURE 1. Framework of IoT

The Internet of Medical Things (IoMT): IoMT is a relatively new development that is part of the Internet of Things (IoT). It is a setting in which numerous healthcare devices, such as smart glucometers, smart blood pressure displays, smart bands, Intelligent pacemakers, and Intelligent pulse rate monitors, are linked and interact with one another to distribute sensitive healthcare officials, hospitals, and doctors to provide exceptional medication and support. The gateway stores these confidential data in some data centres before sending them to the appropriate end users Figure 2 depicts an IoMT architectural design that connects various medical smart appliances and interacts with clinicians to provide effective treatment and assistance.

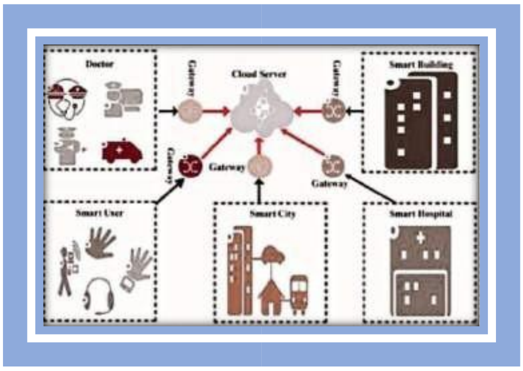


FIGURE 2. IoMT architecture

With the introduction of the IoMT, remote patient monitoring has become more widespread. Connecting outpatients to their doctors and allowing for the secure transfer of health information helps reduce unnecessary hospital visits and the strain on healthcare systems by providing information via a secure web[6]. At the moment, this is critical due to the worldwide pandemic, COVID-19, which is limiting in-person medical appointments and thus preventing the spread. As a result, any cyber attack could have disastrous consequences, putting patients' lives in danger and impeding the widespread adoption of IoMT. Hackers are also motivated by technological advancements to break into the servers that house this sensitive data. A variety of attack vectors could be used to gain control of these intelligent medical devices. For example, if an intruder obtains intelligent pacemakers, he will be able to catch the patient off guard, possibly resulting in death. These emerging risks have the potential to harm the IoMT ecosystem and must be addressed as soon as possible. The IoMT is not only transforming the healthcare industry; it is also enabling a more humane approach to patient healing and care. Nonetheless, it is vulnerable to a wide range of cyber-attacks and vulnerabilities. Several causes for the high number of cyber attacks in IoMT have been identified by the authors, including the following:

- ➢ Issues of compatibility and complexity that arise when a large number of devices and diverse networks are linked.
- ➢ Medical Things is primarily concerned with the exchange of sensitive patient information.

- As a burgeoning paradigm, healthcare decision-makers are rapidly adopting IoMT solutions without regard for security concerns. As a result, new concerns about confidentiality, integrity, and availability (CIA) emerge.
- Application risks such as authorization and authentication breaches, as well as the application's overall security and availability, are also major concerns.
- Certain security computations necessitate a significant amount of computing power.
- IoMT is vulnerable to WSN security violations because the majorities of IoT components receive and transmit data wirelessly. These are just a few of the main reasons why IoMTs are vulnerable to a wide range of harmful attacks.

As a result, it is critical to discuss how to identify and protect against medical equipment assaults. While the majority of IoT vulnerabilities also apply to IoMTs, some are much more specifically targeted at IoMTs due to the sensitive nature of healthcare data. These attacks include, but are not limited to, data breaches, man-in-the-middle attacks, probe attacks, network communication decryption, DoS attacks, and privacy and security concerns. Artificial intelligence can be used to detect and compensate for such attacks in cyber-physical networking systems, as demonstrated by an interesting presentation of research findings in [7]. The type of prevention model also depends on the application; for example, [8] provided an example of smart farming, whereas [9] discovered a research model for intelligent transportation. Some of the most effective solutions focus on dedicated models of user authentication, which are critical in IoT systems where multiple devices must connect to maintain production or delivery systems. In any case, the model must be tailored to the infrastructure it is intended to safeguard. Safe information processing necessitates a high level of security to protect cyber-physical infrastructure from damage. A security framework for energy IoT cyber-physical infrastructures was developed and proposes a comprehensive discussion of networking threads and prevention models. Let us now delve a little deeper into recently developed intelligent malware detectors. The following capabilities distinguish the proposed approach. 1) Extremely high accuracy in detecting various attacks within IoT networks. 2) The ability to detect attacks over time, including right at the start of an attack. 3) The marginal false-positive (FP) rate concerning the detection module ensemble.

2. RELATED WORKS

Azmoodeh et al. [10] proposed a DL-based approach that extracts a graph of executable file operation codes to aid in malicious activity detection. They then presented a feature selection method and used it to generate an adjacency matrix of extracted graphs before training a recurrent neural network (RNN) to distinguish between malicious and benign applications. This method requires a binary executable as input. Aminanto et al. [11] proposed a deep feature extraction and selection model based on deep autoencoders to improve the security of wireless IoT networks. Diro and Chilamkurti [12] presented an LSTM-based model for distributed cyber-attack detection in fog-tothings communication to improve scalability and robustness. On the ISCX and AWID data sets, they reportedly achieved an accuracy rate of 99.91% and 98.22%, respectively. This method has not been suggested for use with Modbus network traffic. Furthermore, the proposed method takes into account a network session window to improve the detection rate and reduce false alarms. The authors of [13] presented a privacy preserving framework for IoMT applications, data collection, and analysis. FFDNN is combined with the FBFSA on the NSL-KDD datasets to detect anomaly incursion in wireless networks. The algorithm selects the best feature with the least amount of redundancy for wireless networks. It consists of three deep layers and a soiree of 30 neurons. This article divides the data into training and testing segments, yielding a 99.69 percent accuracy. We take a different approach to cryptographic security solutions in this study, presenting the detection of intrusion solutions based on ML and DL for detecting cyber-attacks in IoMT. While there is extensive research on using cryptography to detect IoMT attacks, research on intrusion detection in IoMT is still in its early stages, and to the best of our knowledge, no research on using wrapper-based PSO feature selection to improve IDS performance in IoMT exists.

3. PROPOSED METHODOLOGY

This section investigates various methods and algorithms for classifying attack occurrences in the IoMT environment. A thorough examination of the pre-processing phase, feature selection using theswarm intelligence method known as particle swarm optimization (PSO), and classification using GRU, RF, DT, and RNN. Figure 3. Shows the frame of the proposed MDI

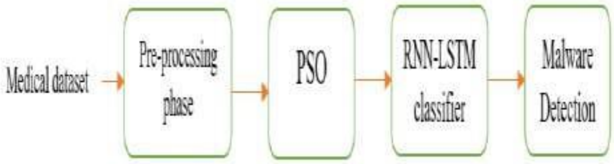


FIGURE 3. Framework of MDI

Pre-processing phase: The algorithm starts by determining whether the received record is complete or contains a missing value (s). If the received record is complete, insert it into the entire dataset to ensure that the IoMT application works properly. Otherwise, the received record may contain one or more missing pieces of information. To train a deep learning neural network, the proposed algorithm divides the entire dataset into training, testing, and validation datasets. 70% of the total data is used for training, while testing and validation datasets each receive 15% of the total data. The trained LRNN predicts missing values and inserts the completed record back into the full dataset. While the process is incomplete, it is repeated.

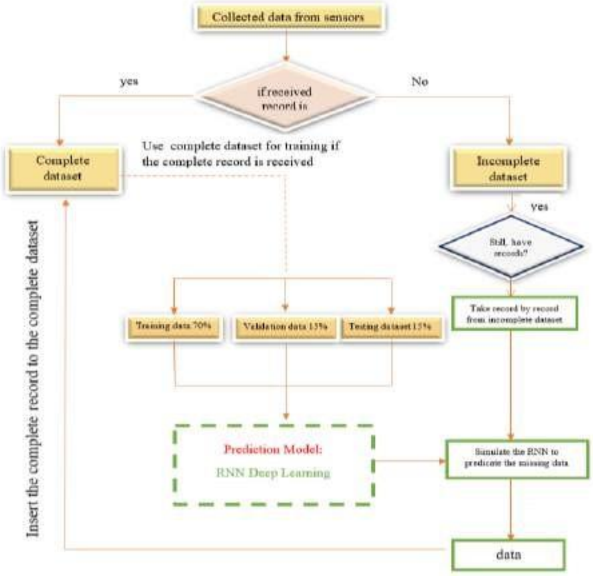

Collected data from sensors
yes
if received record is
No
Use complete dataset for training if the complete record is received
Complete dataset
Incomplete dataset
yes
Still, have records?
Training data 70%
Validation data 15%
Testing dataset 15%
Take record by record from incomplete dataset
Prediction Model:
RNN Deep Learning
Simulate the RNN to predicate the missing data
data
Insert the complete record to the complete dataset

FIGURE 4. Pre-processing phase of MDI

Feature selection: Feature Selection (FS) is a method for selecting and deleting a subset of relevant traits from a large amount of superfluous and repeated data in order to create efficient learning methods. The process of removing redundant and irrelevant attributes from a dataset to improve training achievement in terms of detection accuracy and model construction time is known as FS [14]. Aside from replica complexity, feature selection can aid in the elimination of certain computations [15]. Feature Selection Procedure: Figure 4 depicts the four-stage process of FS techniques. In this study, the PSO is used for FS to choose twenty-one (21) attributes from the forty (40) attributes with one class from the NSL-KDD dataset.

- The production process sequence for the future applicant subgroup
- Its estimation function can estimate the subgroup.
- Criteria for deciding when to stop
- The subgroup is validated using the acceptance procedure.

Particle Swarm Optimization: Eberhart and Kennedy presented a method of optimization called PSO in 1995, which was inspired by animal behaviour. A swarm of particles continuously explores a problem's search area to determine the global best configuration. PSO has been applied to an increasing number of complex, real-world optimization problems since its inception in 1995, where standard methods either underperform or have limited utility. Its visually simple form and few adjustable parameters make it ideal for a wide range of problems that require some degree of approximation. The PSO was adopted to select the dataset's significant features of the attacks.

Overview: The IoMT ecosystem is made up of various sensors that monitor patients' health and send periodic pdates to the cloud Clinicians who can keep their distance. These devices are intelligent enough to collect subtle data and send it to a storage location such as a cloud server; however, they are not intelligent enough to determine whether the data is being conveyed safely or whether any assailants have infringed before and during storage while interacting with the physician in the clinic.

The proposed method consists of a stack of deep RNNs trained on the prepared data set and a DT that aggregates the RNN output. Models of the LSTM deep RNNs are a fundamental class of DL models proposed for learning tasks on sequential data. Despite RNNs' significant ability to learn from sequential information, they suffer from missing data dependency during long-term data patterns

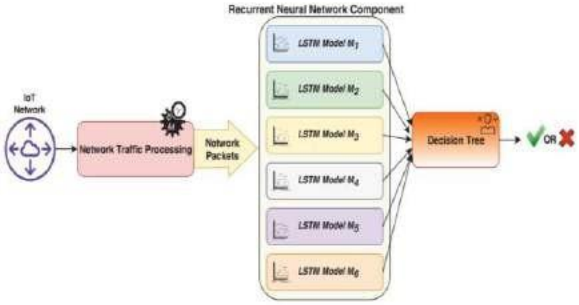


Figure 5: Proposed method overview.

Gated Recurrent Units (GRU): The Gated Recurrent Units (GRU) concept is newer than the LSTM. In general, it is more efficient and, unlike the LSTM, it trains models faster. The model is easily manipulated, and modifications can be performed on it. However,[16] when more memory is required, the LSTM outperforms the GRU. Finally, performance comparisons are largely determined by the type of dataset used. Although the LSTM and GRU have some similarities, there are some important differences that should be mentioned and remembered.

- ➢ The GRU is made up of two gates, whereas the LSTM is made up of three gates.
- ➢ GRUs lack internal memory, which is in contrast to the visible hidden state, and the output gate, which is present in LSTMs, is absent from GRUs.
- ➢ Unlike LSTMs, second nonlinearity is not used when computing GRU output.

Random forest: RF is a group learning method used to improve classification accuracy. An RF consists of several decision trees. RF has a low classification error when compared to other classification techniques. The RF generates a large number of classification trees[17]. The tree is constructed using a tree classification method and bootstrap samples extracted from the original data. Random Forest generates each tree by taking a random sample from the original data and applying a tree classification method.

Decision Tree: The confidence rate of the ith LSTM trained model for class c is denoted by LSTMi,c. The DT accepts these assurance rates as inputs and learns the correlation between the confidence rate of LSTMs and the true label of network traffic hierarchically. Figure 6 shows a schematic representation of a DT component's work in the proposed method. In other words, DT identifies the manifold of the LSTMs' output space and provides us with an explainable model to choose the final label.

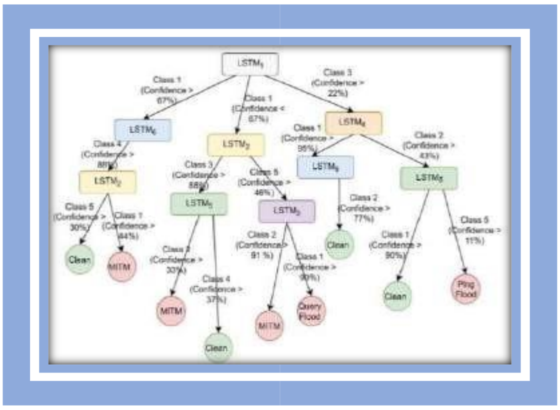

LSTM$_1$
Class 1 (Confidence > 67%)
Class 1 (Confidence < 67%)
Class 3 (Confidence > 22%)
LSTM$_6$
LSTM$_2$
LSTM$_4$
Class 4 (Confidence > 88%)
Class 3 (Confidence > 88%)
Class 5 (Confidence > 46%)
Class 1 (Confidence > 95%)
Class 2 (Confidence > 43%)
LSTM$_2$
LSTM$_5$
LSTM$_3$
LSTM$_6$
LSTM$_5$
Class 5 (Confidence > 30%)
Class 1 (Confidence > 44%)
Class 3 (Confidence > 33%)
Class 4 (Confidence > 37%)
Class 2 (Confidence> 91 %)
Class 1 (Confidence > 90%)
Class 2 (Confidence > 77%)
Class 1 (Confidence > 90%)
Class 5 (Confidence > 11%)
Clean
MITM
MITM
Clean
MITM
Query Flood
Clean
Clean
Ping Flood

FIGURE 6. Schematic view of DT in the proposed method.

Recurrent neural network model: RNN is among the classes of artificial neural networks (ANN) in which node-to-node connections produce a graph directed along a temporal order, allowing for the display of dynamic behaviour. It is also a type of cutting-edge ANN with directed memory cycles. Figure 7. Depicts the architecture model that we developed during our research.

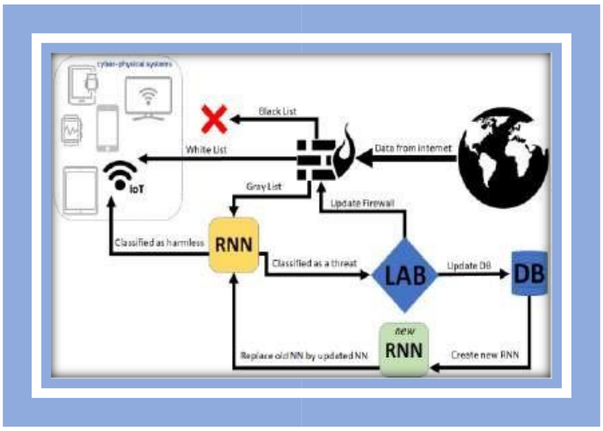


FIGURE 7. Networking thread detection model-based IoT cyber physical devices connected to the network by the use of Recurrent Neural Network

Lstm [Long Short-Term Memory]: LSTM is a fundamental and widely used RNN architecture capable of recognizing patterns. The relationship between the sequence of input data and learning the long-term pattern of data. The structure of an LSTM cell is depicted in Fig. 5. An LSTM is made up of cells, and each cell has three main layers: a forget gate, an input gate, and an output gate. The forget gate is in charge of erasing previous information and its functions are as follows:

$$f_t = \sigma(w_f[h_{t-1}, x_t] + b_f)$$

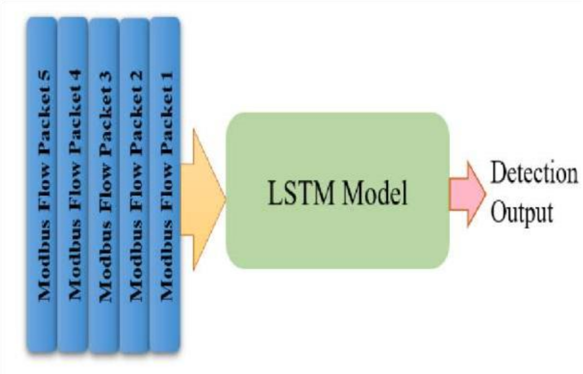


Figure 8: LSTM for an input window size of five packets.

4. RESULTS

Evaluation metrics

✓ Accuracy: A subset of the model's performance was used to assess the model's accuracy. The equation represents   the estimation of

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$$

✓ Recall: recall which denotes the total positives in the classification states versus the precise total of positives in the data, is the total positives in the scheme states versus the precise total of positives in the data. The recall rate is shown in the equation

$$\text{Recall} = \frac{TP}{TP+FN}$$

- ✓ F1-Score: The F1 score can also be used to estimate model performance. It is the weighted average of the model's recall and precision. The value of the F1 Score is given in the equation

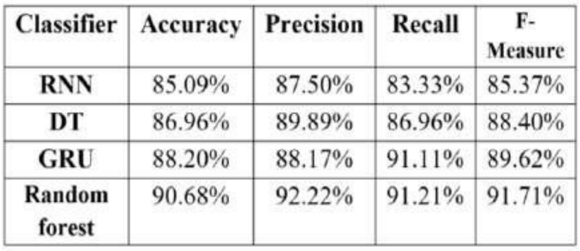
$$\frac{2*TP}{2*TP+FP+FN}$$

In this section, we assess the performance of cutting-edge classification algorithms on the prepared data set. Then, we describe the performance of various LSTMs in detecting cyber-attacks of IoMT findings to demonstrate the robustness of the proposed approach for detecting IoMT cyber-attacks using network traffic. We also discuss the proposed system's training and inference times. Using the LSTMRNN algorithm, we evaluate the effectiveness of our approach and obtain an accuracy rate of over 99% in the detection of cyber-attacks against IoMT devices.

LSTM: In the first stage of our research, we train and evaluate a set of LSTMs to detect IoMT cyber-attacks using network traffic. We train six different LSTMs with different structures on seven different window sizes. The time has come to train a deep learner .is 200, and the batch size is set to 1024. We also make use of the Adam optimizer. To analyse the first stage of our proposed method, we monitor the performance metrics during our experiments fig 6 show how LSTMs decision tree perform in classifying Modbus network traffic for accuracy of various classes The below tables conclude the accuracy of different classifiers:

Recurrent Neural Network : RNN, a feed-forward neural network variant, prefers to work with sequential data. The term "recurrent neural networks" refers to the fact that they perform the same task for each component of categorization, with the outcome dependent on the computation that came before RNNs are particularly well-suited for simulating sequences because they contain cyclic connections.

TABLE 1. Performance of the proposed models Comparative summary



Classifier	Accuracy	Precision	Recall	F-Measure
RNN	85.09%	87.50%	83.33%	85.37%
DT	86.96%	89.89%	86.96%	88.40%
GRU	88.20%	88.17%	91.11%	89.62%
Random forest	90.68%	92.22%	91.21%	91.71%

Deep Recurrent Neural Network Experimental Analysis Table 2 shows that the PSO-RNN had an accuracy of 96.08%, a recall of 85.63%, a precision of 85.63%, and f-measure of 98.15.

TABLE 2. Classifications of Proposed Approaches

Proposed approaches	Accuracy	Recall	Precision	MCC
PS0-RF	99.75	96.59	99.85	99.59
PSO-DT	99.52	96.37	99.59	99.13
PSO-RNN	98.99	93.23	98.90	97.72
PSO-GRU	97.89	91.33	97.56	96.19

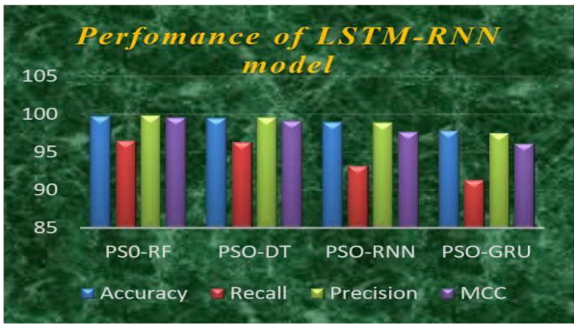


FIGURE 9. Performance of the LSTM-RNN model3

5. CONCLUSION

The study presents a classification model based on RNN and LSTM for identifying intruder assaults in the IoMT environment using benchmarked NSLKDD datasets, which include DoS attacks, probing attacks, u2R attacks, and remote to local assaults. The resampled data set is then lowered using PSO to reduce attribute dimension and identify the most important features. Following that, the reduced data set is classified using a variety of cutting edge ML algorithms such as RF, DT, GRU, LSTM and RNN. Our findings demonstrated the potential of our approach in an IoMT system, where using the DT as an aggregator provides an explainable structure to improve the transparency of the proposed method. We recommend combining the developed RNN-LSTM classifier with the numerical experiments, such a model achieved up to 99.9957% efficiency, as shown in the results. Our solution is not only extremely efficient, but it also requires very little computing power after training and thus consumes very little energy. Because the time it takes for data to pass through the network is measured in nanoseconds, this system can run in the background without interfering with user convenience. We will conclude the ability of LSTM models in the future to propose a more transparent DL model for detecting IoMT cyber-attacks, particularly those in adversarial settings (e.g., battlefields).

ACKNOWLEDGMENT

I am delighted to express my heartfelt appreciation to our department's head, staff, family, and friends. This paper is made possible by their encouragement, assistance, and support.

REFERENCES

[1]. J. Rosen and B. Hannaford, ``Doc at a distance,'' *IEEE Spectr.*, vol. 43, no. 10, pp. 34_39, Oct. 2006.

[2]. K. K. Patel and S. M. Patel, ``Internet of things-IoT: Definition, characteristics, architecture, enabling technologies, application & future challenges,'' *Int. J. Eng. Sci. Comput.*, vol. 6, no. 5, 2016.

[3]. A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, ``Internet of Things for smart cities,'' *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22_32, Feb. 2014.

[4]. E. B. Karbab, M. Debbabi, A. Derhab, and D. Mouheb, ``Android malware detection using deep learning on API method sequences,'' Dec. 2017, *arXiv:1712.08996*. [Online]. Available: https://arxiv.org/abs/1712.08996

[5]. S. Jabbar, K. R. Malik, M. Ahmad, O. Aldabbas, M. Asif, S. Khalid, K. Han, and S. H. Ahmed, ``A methodology of real-time data fusion for localized big data analytics,'' *IEEE Access*, vol. 6, pp. 24510_24520, 2018.

[6]. F. Ullah, J. Wang, M. Farhan, M. Habib, and S. Khalid, ``Software plagiarism detection in multi programming languages using machine learning approach,'' *Concurrency Comput., Pract. Exper.*, to be published.

[7]. M. Egele, T. Scholte, E. Kirda, and C. Kruegel, ``A survey on automated dynamic malware-analysis techniques and tools,'' *ACM Comput. Surv.*, vol. 44, no. 2, p. 6, Feb. 2012.

[8]. I. Gha_r, J. Saleem, M. Hammoudeh, H. Faour, V. Prenosil, S. Jaf, S. Jabbar, and T. Baker, ``Security threats to critical infrastructure: The human factor,'' *J. Supercomput.*, vol. 74, no. 10, pp. 4986_5002, Oct. 2018.

[9]. A. Moore, *Intellectual Property and Information Control: Philosophic Foundations and Contemporary Issues*. Abingdon, U.K.: Routledge, 2017.

[10]. A. Azmoodeh, A. Dehghantanha, and K. R. Choo, “Robust malware detection for Internet of (battlefield) Things devices using deep eigenspace learning,” *IEEE Trans. Sustain. Comput.*, vol. 4, no. 1, pp. 88–95, Jan.–Mar. 2019.

[11]. A. Diro and N. Chilamkurti, “Leveraging LSTM networks for attack detection in fog-to-things communications,” *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 124–130, Sep. 2018.

[12]. L. Nataraj, S. Karthikeyan, G. Jacob, and B. S. Manjunath, ``Malware images: Visualization and automatic classification,'' in *Proc. 8th Int. Symp. Vis. Cyber Security.*, Jul. 2011, p. 4.

[13]. A. Makandar and A. Patriot, `Malware class recognition using image processing techniques,'' in *Proc. Int. Conf. Data Manage., Anal. Innov. (ICD- MAI)*, Feb. 2017, pp. 76_80

[14]. I. Lokshina and C. Lanting, ``A qualitative evaluation of IoT-driven eHealth: Knowledge management, business models and opportunities, deployment and evolution,'' in *Data-Centric Business and Applications* (Lecture Notes on Data Engineering and Communications Technologies), vol. 20, N. Kryvinska and M. Gregu², Eds. Cham, Switzerland: Springer, 2019, doi: 10.1007/978-3-319-94117-2_2.

[15]. E. K. Wang, C.-M. Chen, M. M. Hassan, and A. Almogren, ``A deep learning based medical image segmentation technique in Internet- Medical-Things domain,'' *Future Gener. Computer. Syst.*, vol. 108, pp. 135_144, Jul. 2020, doi: 10.1016/j.future.2020.02.054.

[16]. H. Sedjelmaci, M. Hadji, and N. Ansari, “Cyber security game forintelligent transportation systems,” IEEE Network, vol. 33, no. 4, pp. 216–222, 2019.