Cyber Threat Detection on Internet of Things

1st Mebiratu Beyene Bekele
ICT4D Research Center
Bahir Dar institute of Technology, Bahir Dar University
Bahir Dar, Ethiopia
https://orcid.org/0000-0001-8320-775X

2nd Yesuneh Getachew Taye
ICT4D Research Center
Bahir Dar institute of Technology, Bahir Dar University
Bahir Dar, Ethiopia
yesu397@gmail.com

3rd Ephrem Getachew Demesa
Tallinn University of Technology
ephrem.demesa@gmail.com

***Abstract*—The internet of things (IoT) is a connected network of devices that has the ability to communicate with each other and bring data to users using internet. The amount of collected data from IoT in different domain is so huge and conventional analysis of these data is very hard and need more feasible methods. There are huge calls in IoT for appropriate security and privacy policies to prevent potential cyber threats. One of the security requirements of the IoT user is the confidentiality and integrity of the data collected by the sensors. Recently deep learning is prominent approach to combat intrusion in IoT and several deep learning models have been proposed for it. However, the field is still evolving and there is ongoing research to further improve the performance of the system. We have selected deep learning algorithms like LSTM, AUC, GRU, RNN and MLP and compared with other state of art methods like CNN , SVM and others. The models RNN, LSTM and GRU, an Accuracy of 100%, recall of 100%, and precision of 100% were recorded. Compared with AUC and MLP , the RNN, LSTM and GRU records higher in accuracy, recall and precision.**

***Index Terms*—Intrusion detection, Cyber-attack, Internet of things, Deep Learning**

I. Introduction

The IoT is a connected network of devices which have ability to communicate with each other and bring data to user using internet. The advancement of IoT in recent years is due to its broad applicability, scalability and smartness [1] [2]. The amount of data collected from IoT is so huge that conventional analysis of these data is very hard and need more feasible methods [2] [3]. Furthermore, the data are rising all the time. It requires a great demand for efficient data mining techniques in order to help identify IoT patterns, catch fraudulent activities, make better use of resources and improve the quality of service [4] [5] [6]. Recently huge call in IoT for appropriate security and privacy policies to prevent potential cyber threats.
The IoT data are generated from various IoT devices such as Low-cost digital sensors like temperature and humidity, ultrasonic sensor, water level detection sensor, pH sensor meter, soil moisture sensor, heart rate sensor and flame sensor. One of the security requirements of the IoT user is the confidentiality and integrity of the data collected by the sensors. Significant work has been done by the cyber security community in creating sophisticated security tools and techniques for protecting users and data in traditional IT systems. Yet, these measures themselves cannot be immediately deployed for IoT/industrial IoT (IIoT) based systems regardless of its different characteristics. Furthermore, with novel threats that can potentially breach IoT networks, in which existing techniques are insufficient to address them. It becomes necessary to investigate deep into advanced forensic approaches to detect and investigate malicious behavior, which are broadly applied to investigate network traffic and detect contaminated devices participating in IoT network [8].
An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. It searches for known threats and suspicious or malicious activity, and sends alerts to IT and security teams when it detects any security risks and threats [9] [10]. Several deep learning models have been proposed for IoT like Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) and Gated Recurrent Units (GRUs) [11] [12] [13].
The research conducted on these models has shown that deep learning-based intrusion detection systems can achieve high accuracy in detecting intrusions in IoT. However, the field is still evolving, and there is ongoing research to further improve the performance of these systems. The effectiveness of the systems.

II. Related works

We have performed widespread survey on existing literature to identify related works and research gap thereof.

A. Intrusion detection systems

An IDS is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system [14]. There are several types of IDS:

- Network Intrusion Detection System (NIDS): This type of IDS is deployed at strategic points within an organization's network to monitor incoming and outgoing traffic

- Host Intrusion Detection System (HIDS): This system is installed on individual devices that are connected to the internet and an organization's internal network.
- Signature-based Intrusion Detection System (SIDS): This type of IDS monitors all packets on an organization's network and compares them with attack signatures on a database of known threats.
- Anomaly-based Intrusion Detection System (AIDS): This solution monitors traffic on a network and compares it with a predefined baseline that is considered "normal".

B. Cyber attack detection on IoT

The cyber-attack is becoming one of the most severe threats to IoT security. These attacks occur in many ways and typically target anomalous assets, affecting one or more IoT devices that can be used as resources or platforms. As a result, securing IoT devices and designing intrusion- resistant IoT networks become increasingly important to safeguard data [15]. The problem is how to effectively detect and prevent intrusions in time is very challenging.

Conventional IDS like signature or rule-based approaches have not been adequate for the fast-growing network and unable to deal with attacks of their growing volume, complexity and deflation. Therefore, artificial intelligence techniques have been integrated into all aspects of the IoTs and making more comfortable in various ways. Researcher [15] proposed a novel deep learning model DIDS incorporates the prediction of unknown attacks to handle the computational overhead in large networks and increase the throughput with a low false alarm rate.

Amjad Rehman et.al [16] provided an inclusive analysis of intrusion detection based on deep learning techniques by using public network-based datasets of IDS (NB15 and KDD99). The accuracy in KDD99 and UNSWNB15 datasets was shown 99.996% and 89.134%. Abdelghani D et.al [17] proposed a novel framework to improve IDS performance based on the data collected from the IoT environments. The developed framework relies on deep learning and metaheuristic (MH) optimization algorithms to perform feature extraction and selection. The researchers used KDDCup-99, NSL-KDD, CICIDS-2017, and BoT-IoT. Intrusion Detection in IoT Networks Using Deep Learning Algorithm proposed for detecting denial-of-service (DoS) attacks [18]. The researcher incorporated the evaluation of RF, CNN and MLP algorithms. Alaa M et.al [19]explored intrusion detection methods implemented using deep learning, compares the performance of different deep learning methods, and identifies the best method for implementing intrusion detection in IoT. This research is conducted based on CNNs, LSTM, and GRU. This method seemed to have the highest accuracy compared to the existing methods. Ayesha S et.al [20] proposed a deep learning approach for intrusion detection in IoTs using focal loss function. The focal loss function facilitates optimization of the model by enabling dynamically scaled-gradient updates leading to down-weighing easy instances and forcing the model to focus on the hard misclassified examples. Researcher implemented focal loss function in two well-studied Deep Learning algorithms (FNN and CNN). The CNN trained using focal loss function performed better with respect to accuracy, precision, F1 score and MCC score. The below Table 1 shows summary of related research work so far done.

TABLE I
SUMMARY OF RELATED WORK

Author(s)	*Model*	*Dataset*	*Accuracy*
[15]	Random forest and TabNet	NSL-KDD and KDD-CUP 0.99	0.95 && 0.96
[18]	CNN, and MLP	BoT-IoT	0.987 && 0.79
[14]	LSTM-RNN	KDD Cup 1999	0.98
[21]	DL-Sim, DLTestbed and WC	CC2650	0.96, 0.93 && 0.98
[22]	DNN	NSL-KDD	0.98
[23]	AE	KDD99	0.99
[24]	BLSTM RNN	UNSWNB15	0.95
[25]	RFC	NSL-KDD &&UNSW-NB 15	0.99
[26]	EIDM	CICIDS2017	0.95
[27]	LSTM and GRU	DARPA/KDD Cup 99	0.98

III. DEEP LEARNING MODEL

In this section, we discuss about the nature of Edge-IIoTdataset, preprocessing technique, feature selection, hyper parameter tuning, deep learning algorithm, the architecture of proposed model and performance evaluation metrices has been described in detail.

A. Understanding the Edge-IIoTdataset

The Edge-IIoTset is a comprehensive and realistic cyber security dataset of IoT and IIoT applications. It's designed for use machine learning-based IDS in two different modes: centralized and federated learning. [28].

The dataset was generated using IoT/IIoT testbed with a large representative set of devices, sensors, protocols and cloud/edge configurations. The sensor devices in participated in data generation are 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. The Edge-IIoTset identified and analyzed fourteen attacks related to IoT and IIoT connectivity protocols, which are categorized into five threats, including, DoS/DDoS attacks, information gathering, man in the middle attacks, injection attacks and malware attacks.The below figure 1 shows attack type in dataset.

B. Data Preprocess

Pre-processing the Edge-IIoTset dataset involves several steps.

1) Loading the Dataset: The dataset is loaded into a panda DataFrame using the readcsv function. Data shape is (2219201, 63)): 2219201 rows of record and 63 features. The below figure 2 shows attack type and data distribution.

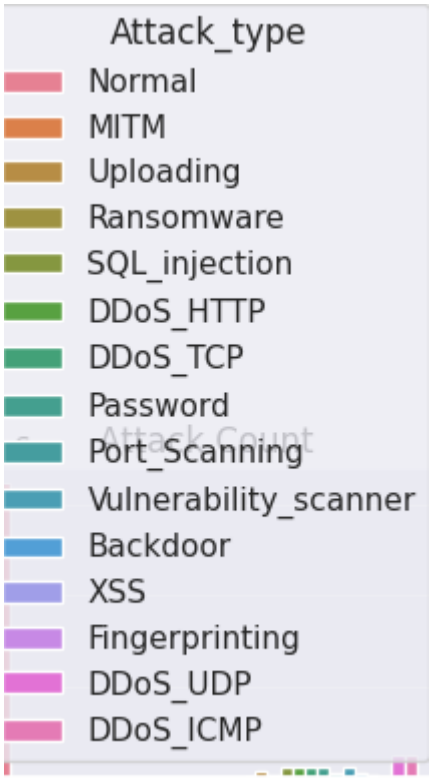

Fig. 1. Attack type in dataset

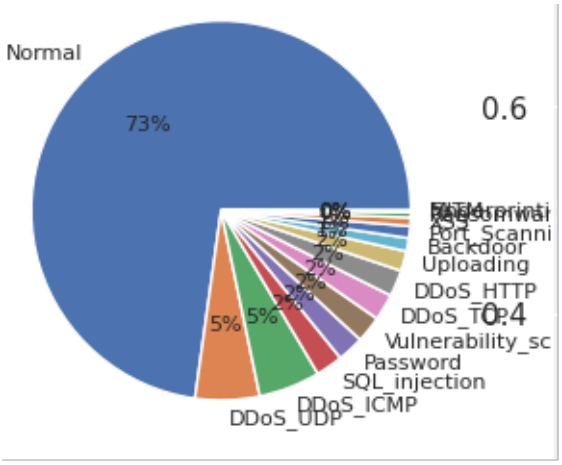

Fig. 2. Bar chart for data distribution based on normal and attack type

2) Data Cleaning: Unnecessary columns are dropped, and any rows with missing values are removed.

3) Data Shuffling: The dataset is shuffled to ensure that the training/test splits contain a representative mix of examples.Shuffle the rows of the DataFrame to introduce randomness

4) One-Hot Encoding: Categorical features are one-hot encoded

C. Deep learning Algorithms

Deep learning is one of the machine learning techniques that learns features directly from data. When the amount of data is increased, machine learning techniques are insufficient in terms of performance and deep learning gives better performance like accuracy. We have used five DL algorithms for model development.

Recurrent Neural Network (RNN): Type of artificial neural network that is primarily used for processing sequential data or time series data. Unlike traditional feedforward neural networks, RNNs have "memory" in the sense that information from prior inputs can influence the current input and output. This makes RNNs particularly useful for tasks such as language translation, speech recognition, intrusion detection and image captioning. In contrast to the uni-directional feedforward neural network, an RNN is a bi-directional artificial neural network, meaning that it allows the output from some nodes to affect subsequent input to the same nodes [29]. One distinguishing characteristic of RNNs is share parameters across each layer of the network. While feedforward networks have different weights across each node, RNNs share the same weight parameter within each layer of the network.

Gated Recurrent Unit (GRU): It's designed as a simpler alternative to LSTM networks. Like LSTM, GRU can process sequential data such as text, speech, and time-series data. The key idea behind GRU is to use gating mechanisms to selectively update the hidden state of the network at each time step [30].

Autoencoder (AUC): A type of artificial neural network used to learn efficient coding of unlabeled data, which is a form of unsupervised learning. The aim of an autoencoder is to learn a lower-dimensional representation (encoding) for higher-dimensional data, typically for dimensionality reduction [31] [32]. An autoencoder learns two functions: An encoding function that transforms the input data and a decoding function that recreates the input data from the encoded representation.

Multilayer Perceptron (MLP): A type of feedforward artificial neural network that consists of fully connected neurons with a nonlinear kind of activation function. It's organized in at least three layers: an input layer, one or more hidden layers, and an output layer [33] [34]. MLP is robust and complex architecture to learn regression and classification models for difficult datasets. MLPs form the basis for all neural networks and have greatly improved the power of computers when applied to classification and regression problems.

LSTM: The LSTM network is composed of a cell, an input gate, an output gate, and a forget gate. The cell remembers values over arbitrary time intervals, and the three gates regulate the flow of information into and out of the cell [35]. One of the advantages of LSTM networks is their ability to remember inputs over a long period of time, which makes them particularly useful for tasks such as language translation, speech recognition, and image captioning.

D. Model development

The model development is training a deep learning algorithm to predict the class from the features, tuning it for the business need, and validating it on holdout data. The output from modeling is a trained model that can be used for inference, making predictions on new data points. The purpose of the proposed intrusion detection model in IoT is to detect intrusion in data that is being exchanged by IoT devices. The model takes data from IoT devices as an input, systematically process input data, and produce predictions of two folds; "normal" or "attack". Figure 3 provides a high-level view of the model design.

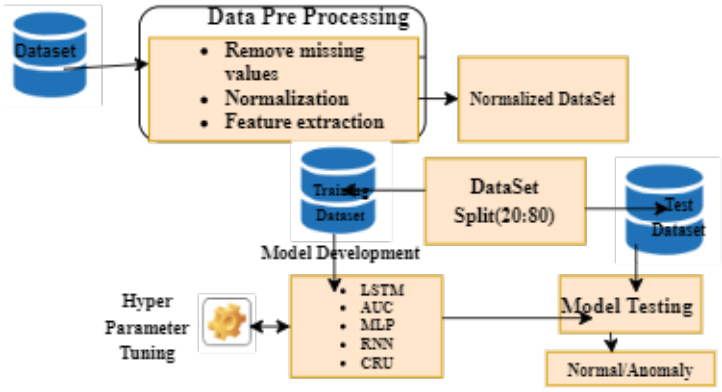

Fig. 3. Proposed model design

E. Evaluation Criteria and Metrics

Precision measures the proportion of true positives (correctly predicted positive instances) out of all the instances that the model predicted as positive (true positives + false positives). Recall measures the proportion of true positives (correctly predicted positive instances) out of all the actual positive instances (true positives + false negatives). Accuracy measures the proportion of correctly classified instances out of all the instances that the model predicted. Mean Squared Error (MSE) represents the average of the squared difference between the original and predicted values in the dataset. It measures the variance of the residuals. Root Mean Squared Error (RMSE) is the square root of mean squared error. It measures the standard deviation of residuals.

F. Experiment

1) Experimental Setting: In this study, we conducted the experiment in five different deep learning models with hyper parameter tuning. The experiments were conducted using a Edge-IIoTset dataset, which had 2,219,201 instances [6]. We used manual hyper-parameter tuning for each algorithm to select the parameters values. The specified hyper-parameter values provided are shown in Tables 2. We also applied data pr-eprocessing techniques i.e., filling the missing values using forward fill, splitting the dataset to 80/20 % training and testing and applying one hot encoding. The researcher implements model based on TensorFlow and Keras libraries. The RMSE, MSE, precision, recall and accuracy were used to evaluate the model performance.

TABLE II
PARAMETERS USED FOR MODELS

Parameters	*LSTM*	*RNN*	*AUC*	*MLP*	*GRU*
Neurons	50	50	50	50	50
Epochs	4	4	4	4	4
Optimizer	adam	adam	adam	adam	adam
Batch size	1000	1000	1000	1000	1000
Learning rate	0.0001	0.0001	0.0001	0.0001	0.0001

2) Model development: We have selected five algorithms namely LSTM, GRU, AUC, RNN and MLP. The detail experimentation and code are available on my GitHub page.

3) Experimental results: We conducted five experiments to develop the intrusion detection model for IoT. After the predictive model has been developed, an experiment has been carried out to evaluate how effectively it detects and identifies intruders in the Edge IOT/IIOT dataset. To this end, experiments are conducted for each deep learning approach with all features. In each experiment the deep learning algorithms LSTM, GRU, RNN, AUC and MLP to select the best performer for detection of intruder in the Edge IOT/IIOT dataset. The table 3 and figure 4 below shows performance of models.

TABLE III
MODEL PERFORMANCE

Model	*Precision*	*Recall*	*Accuracy*	*MSE*	*RMSE*
LSTM	1	1	1	0.00048	0.022
AUC	0.91	0.71	0.83	0.16	0.40
MLP	0.90	0.68	0.82	0.18	0.42
RNN	1	1	1	0	0
GRU	1	1	1	0.0028	0.053

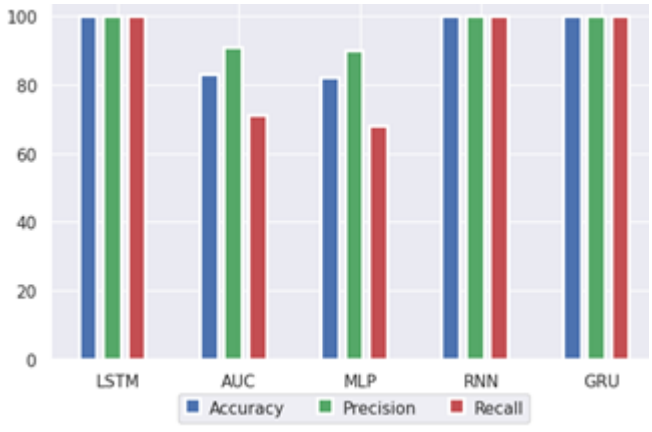

Fig. 4. Model Performance

4) Discussion : In this section, we discussed the experimental result of deep learning for Intrusion Detection on IoTs. Overall, the experiment yielded promising results on intrusion detection on IoT. The table 3 and figure 4 present the findings and their comparison. It indicated that RNN, LSTM and GRU, an Accuracy of 100%, recall of 100%, and precision of 100% were recorded. We have compared selected deep learning method with other state of art methods like CNN , SVM and others. The selected algorithms AUC , MLP , RNN, LSTM and GRU recorded higher in accuracy, recall and precision.

IV. Conclusion and recommendation

The IoT data are generated from various IoT devices such as 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. One of the security requirements of the user of the IoT is the confidentiality and integrity of the data recorded by the sensors. Significant work has been done by the cybersecurity community in creating sophisticated security tools and techniques for protecting user and data. Therefore, artificial intelligence techniques have been integrated into all aspects of the IoTs and making more comfortable in various ways. The main objectives of this study were to improve the accuracy and performance of the deep learning approach and make it easier to detect intrusions. We have selected five algorithms namely LSTM, GRU, AUC, RNN and MLP to enhance intrusion detection in IoTs and compared with other state of art methods. We evaluated the model's performance using recall, precision, accuracy, RSME and MSE. The future works mainly focus on the following aspects: combining different deep learning algorithm with optimization and hyper parameter tuning is next task of researcher should consider.

References

[1] S. Nižetić, P. Šolić, D. López-de-Ipiña González-de-Artaza, and L. Patrono, "Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future," J. Clean. Prod., vol. 274, 2020, doi: 10.1016/j.jclepro.2020.122877.

[2] M. Dachyar, T. Y. M. Zagloel, and L. R. Saragih, "Knowledge growth and development: internet of things (IoT) research, 2006–2018," Heliyon, vol. 5, no. 8, p. e02264, 2019, doi: 10.1016/j.heliyon.2019.e02264.

[3] S. Luthra, D. Garg, S. K. Mangla, and Y. P. Singh Berwal, "Analyzing challenges to Internet of Things (IoT) adoption and diffusion: An Indian context," Procedia Comput. Sci., vol. 125, pp. 733–739, 2018, doi: 10.1016/j.procs.2017.12.094.

[4] A. Shobanadevi and G. Maragatham, "Data mining techniques for IoT and big data - A survey," Proc. Int. Conf. Intell. Sustain. Syst. ICISS 2017, no. Iciss, pp. 607–610, 2018, doi: 10.1109/ISS1.2017.8389260.

[5] P. Sunhare, R. R. Chowdhary, and M. K. Chattopadhyay, "Internet of things and data mining: An application oriented survey," J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 6, pp. 3569–3590, 2022, doi: 10.1016/j.jksuci.2020.07.002.

[6] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning," IEEE Access, vol. 10, pp. 40281–40306, 2022, doi: 10.1109/ACCESS.2022.3165809.

[7] A. Aziz, O. Schelén, and U. Bodin, "A Study on Industrial IoT for the Mining Industry: Synthesized Architecture and Open Research Directions," Internet of Things, vol. 1, no. 2, pp. 529–550, 2020, doi: 10.3390/iot1020029.

[8] P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, "Internet of Things: Security and Solutions Survey," Sensors, vol. 22, no. 19, pp. 1–51, 2022, doi: 10.3390/s22197433.

[9] A. Pinto, L. C. Herrera, Y. Donoso, and J. A. Gutierrez, "Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure," Sensors, vol. 23, no. 5, pp. 1–18, 2023, doi: 10.3390/s23052415.

[10] A. Drewek-Ossowicka, M. Pietrołaj, and J. Rumiński, "A survey of neural networks usage for intrusion detection systems," J. Ambient Intell. Humaniz. Comput., vol. 12, no. 1, pp. 497–514, 2021, doi: 10.1007/s12652-020-02014-x.

[11] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey," Appl. Sci., vol. 9, no. 20, 2019, doi: 10.3390/app9204396.

[12] S. V. N. Santhosh Kumar, M. Selvi, and A. Kannan, "A Comprehensive Survey on Machine Learning-Based Intrusion Detection Systems for Secure Communication in Internet of Things," Comput. Intell. Neurosci., vol. 2023, pp. 1–24, 2023, doi: 10.1155/2023/8981988.

[13] D. H. Lakshminarayana, J. Philips, and N. Tabrizi, "A survey of intrusion detection techniques," Proc. - 18th IEEE Int. Conf. Mach. Learn. Appl. ICMLA 2019, pp. 1122–1129, 2019, doi: 10.1109/ICMLA.2019.00187.

[14] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection," 2016 Int. Conf. Platf. Technol. Serv. PlatCon 2016 - Proc., no. September 2017, 2016, doi: 10.1109/PlatCon.2016.7456805.

[15] B. Madhu, M. Venu Gopala Chari, R. Vankdothu, A. K. Silivery, and V. Aerranagula, "Intrusion detection models for IOT networks via deep learning approaches," Meas. Sensors, vol. 25, no. November 2022, p. 100641, 2023, doi: 10.1016/j.measen.2022.100641.

[16] A. R. Khan, M. Kashif, R. H. Jhaveri, R. Raut, T. Saba, and S. A. Bahaj, "Deep Learning for Intrusion Detection and Security of Internet of Things (IoT): Current Analysis, Challenges, and Possible Solutions," Secur. Commun. Networks, vol. 2022, 2022, doi: 10.1155/2022/4016073.

[17] A. Dahou et al., "Intrusion Detection System for IoT Based on Deep Learning and Modified Reptile Search Algorithm," Comput. Intell. Neurosci., vol. 2022, pp. 1–15, 2022, doi: 10.1155/2022/6473507.

[18] Bambang Susilo, "Intrusion Detection in IoT Networks Using Deep Learning Algorithm," information, p. 11, 2020.

[19] A. M. Banaamah and I. Ahmad, "Intrusion Detection in IoT Using Deep Learning," Sensors, vol. 22, no. 21, 2022, doi: 10.3390/s22218417.

[20] Ayesha S. Dina, "A deep learning approach for intrusion detection in Internet of Things using focal loss function," Internet of Things, vol. 22, 2023.

[21] G. Thamilarasu and S. Chawla, "Towards deep-learning-driven intrusion detection for the internet of things," Sensors (Switzerland), vol. 19, no. 9, 2019, doi: 10.3390/s19091977.

[22] C. Liang, B. Shanmugam, S. Azam, M. Jonkman, F. De Boer, and G. Narayansamy, "Intrusion Detection System for Internet of Things based on a Machine Learning approach," Proc. - Int. Conf. Vis. Towar. Emerg. Trends Commun. Networking, ViTECoN 2019, pp. 1–6, 2019, doi: 10.1109/ViTECoN.2019.8899448.

[23] A. Dawoud, O. A. Sianaki, S. Shahristani, and C. Raun, "Internet of Things Intrusion Detection: A Deep Learning Approach," 2020 IEEE Symp. Ser. Comput. Intell. SSCI 2020, pp. 1516–1522, 2020, doi: 10.1109/SSCI47803.2020.9308293.

[24] B. Roy and H. Cheung, "A Deep Learning Approach for Intrusion Detection in Internet of Things using Bi-Directional Long Short-Term Memory Recurrent Neural Network," 2018 28th Int. Telecommun. Networks Appl. Conf. ITNAC 2018, pp. 1–6, 2018, doi: 10.1109/ATNAC.2018.8615294.

[25] S. Ethala and A. Kumarappan, "A Hybrid Spider Monkey and Hierarchical Particle Swarm Optimization Approach for Intrusion Detection on Internet of Things," Sensors, vol. 22, no. 21, 2022, doi: 10.3390/s22218566.

[26] O. Elnakib, E. Shaaban, M. Mahmoud, and K. Emara, "EIDM: deep learning model for IoT intrusion detection systems," J. Supercomput., vol. 79, no. 12, pp. 13241–13261, 2023, doi: 10.1007/s11227-023-05197-0.

[27] M. K. Putchala, "Deep Learning Approach for Intrusion Detection System (IDS) in the Internet of Things (IoT) Network using Gated Recurrent Neural Networks (GRU)," Wright State Univ., p. 64, 2017, [Online]. Available: https://corescholar.libraries.wright.edu/etdall/1848/

[28] M. A. Ferrag, "Edge-IIoTset Cyber Security Dataset of IoT & IIoT." Accessed: Mar. 02, 2024. [Online]. Available: https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iot-iiot to Cardiovascular ICUs Based on

Clinical Time Series Data †," Eng. Proc., vol. 18, no. 1, pp. 1–10, 2022, doi: 10.3390/engproc2022018001.
[29] B. Cao, C. Li, Y. Song, Y. Qin, and C. Chen, "Network Intrusion Detection Model Based on CNN and GRU," Appl. Sci., vol. 12, no. 9, 2022, doi: 10.3390/app12094184.
[30] E. H. Demircioğlu and E. Yılmaz, "A Method Based on an Autoencoder for Anomaly Detection in DC Motor Body Temperature," Appl. Sci., vol. 13, no. 15, 2023, doi: 10.3390/app13158701.
[31] K. A. Alaghbari, H. S. Lim, M. H. M. Saad, and Y. S. Yong, "Deep Autoencoder-Based Integrated Model for Anomaly Detection and Efficient Feature Extraction in IoT Networks," Internet of Things, vol. 4, no. 3, pp. 345–365, 2023, doi: 10.3390/iot4030016.
[32] R. Qaddoura, A. M. Al-Zoubi, H. Faris, and I. Almomani, "A multi-layer classification approach for intrusion detection in iot networks based on deep learning," Sensors, vol. 21, no. 9, pp. 1–21, 2021, doi: 10.3390/s21092987.
[33] H. Ghani, B. Virdee, and S. Salekzamankhani, "A Deep Learning Approach for Network Intrusion Detection Using a Small Features Vector," J. Cybersecurity Priv., vol. 3, no. 3, pp. 451–463, 2023, doi: 10.3390/jcp3030023.
[34] J. Zhang, X. Zhang, Z. Liu, F. Fu, Y. Jiao, and F. Xu, "A Network Intrusion Detection Model Based on BiLSTM with Multi-Head Attention Mechanism," Electron., vol. 12, no. 19, pp. 1–17, 2023, doi: 10.3390/electronics12194170.
[35] J. Han and W. Pak, "Hierarchical LSTM-Based Network Intrusion Detection System Using Hybrid Classification," Appl. Sci., vol. 13, no. 5, 2023, doi: 10.3390/app13053089.