Int. j. inf. tecnol. (January 2024) 16(1):13–20
https://doi.org/10.1007/s41870-023-01651-7

ORIGINAL RESEARCH

DL-SkLSTM approach for cyber security threats detection in 5G enabled IIoT

Anjali Rajak[1] · **Rakesh Tripathi**[1]

Received: 26 July 2023 / Accepted: 17 November 2023 / Published online: 18 December 2023
© The Author(s), under exclusive licence to Bharati Vidyapeeth's Institute of Computer Applications and Management 2023

Abstract The advancement of 5G technology has enabled the IIoT (Industrial Internet of Things) to integrate artificial intelligence, cloud computing, and edge computing in real-time, leading to an improvement in industrial procedures in terms of efficiency. Despite the benefits of 5G technology for the IIoT, it also introduces new security risks and complexity to the control systems used in these ecosystems. Recent cyber-attacks are increasingly targeting vulnerable IoT devices, highlighting the need for enhanced security and privacy measures. To address this issue, this study proposes a 5G-based system that utilizes the DL-SkLSTM (Deep Learning- Stacked Long Short-Term Memory) based architecture to detect and classify the cyber-attack on a publicly accessible IIoT dataset, namely the Edge-IIoTset. SkLSTM is used to differentiate various cyberattacks. Finally, conducting a comprehensive analysis and comparison, we have identified that the proposed system outperforms several state-of-the-art DL and machine learning techniques.

Keywords 5G · Cyberattack · Deep learning · Cybersecurity · Industrial IoT

1 Introduction

The IoT (Internet of Things), enables both traditional electronics and ubiquitous things to connect to the Internet and exchange data. These things are integrated with sensors, computation, communication, and networking capabilities. It has been utilized in a variety of emerging applications, including smart cities, smart grids, etc. IoT's broad scalability, support for smart applications, and applicability are some of the factors contributing to its recent spectacular rise. Without a doubt, the strength of conventional IoT applications comes from their capacity to collect, analyze, and communicate user data in a ubiquitous and committed way. The IoT network connects sensors and gadgets that are used in various industries, such as manufacturing, healthcare, agriculture, and other smart applications [1]. These systems consist of sensors and smart devices for applications such as mobile application monitoring, home automation, and wearable sensors. Typically, these applications do not result in critical situations in the case of malfunction [4].

The IIoT, on the other hand, is a subset of the IoT and it refers to the use of IoT devices in often confined industrial environments. The industrial revolution, known as Industry 4.0, is made possible in large part by the IIoT [2]. IoT-connected devices already number more than 8 billion, and by 2027, that number is anticipated to rise to 41 billion. With industries including smart home, healthcare, manufacturing, automotive, energy, transportation, logistics, and media at the forefront of IoT growth, the worldwide IoT market was anti-cipated to be over $380 billion in 2022 and is expected to reach over $1.8 trillion by 2028 [3].

The development of wireless connectivity, particularly 5G, is essential for the advancement of technology and automation in manufacturing. The convergence of intelligent technology and the interconnection of IoT devices and sensors can lead to improved operational performance and the development of advanced systems through the integration of software, hardware, data collection, and advanced analytics tools and techniques. This presents significant opportunities for next-generation wireless communications

✉ Anjali Rajak
arajak.phd2021.it@nitrr.ac.in

Rakesh Tripathi
rtripathi.it@nitrr.ac.in

[1] National Institute of Technology Raipur, Raipur, India

and the expansion of the IIoT. In addition, the use of advanced AI (Artificial intelligence) solutions can provide more profound insights and facilitate the development of intelligent and flexible systems, leading to improved operational performance at an industrial level. One of the main challenges associated with implementing IIoT applications is the potential risk to security (i.e., cyber-attacks). The goal of cyberattacks is to gain unauthorized access to network system components by disseminating malicious software. Information gathering, DoS, DDoS, man in the middle (MITM), injection, and malware are examples of these types of attacks [21]. These threats jeopardize the confidentiality, availability, and integrity of data. Thus, security is a key concern holding up the widespread implementation of smart applications. It will be more crucial than ever to create an efficient system control approach that includes assurance and risk assessment as IIoT-based systems become more prevalent. In order to prevent the usage of unreliable devices, the industry must be able to confidently identify IIoT systems. It is essential to have a way to identify each particular sensor, system, and device in order to update or replace lost or outdated systems [16, 17, 22].

In this study, we employed AI to develop a DL-based 5G-enabled industrial Internet of Things cyber-attack detection system. The proposed system utilizes a multilayer LSTM architecture to classify and identify various cyber-attack types. The proposed architecture incorporates a sufficient number of layers that were trained and tested using data from Edge-IIoTset, which is publicly accessible. Moreover, 5G technology, which offers low latency and high throughput capabilities, has been added to the system. By enabling real-time connectivity this approach is more effective than the previous one, which restricted real-time connectivity to private networks with high-speed connectivity. The system can enable real-time communication applications like driverless vehicles and other smart city applications due to the use of 5G technology in it.

The main objective of this study is to highlight the advancements made in the area of attack detection or classification in the IIoT using a DL-based technique.

1. To propose a DL-based stacked LSTM architecture for detecting cyber-attacks in 5G-enabled IIoT.
2. Data preprocessing techniques are used to improve the stacked LSTM architecture's performance. The publicly available Edge-IIoTset dataset is used to train and evaluate the detection system.
3. Examine and compare the outcomes of the proposed system with various deep learning and machine learning models for attack detection in terms of detection rate, precision, and accuracy.

This study is categorized into several sections, starting with Sect. 2, which provides a summary of related work that has been done on attack detection in IIoT applications. Section 3 describes the 5G-enabled system for the IIoT that utilizes DL-based stacked LSTM, for detecting various types of cyber-attacks. The next section describes the Edge-IIoTset dataset used for the experiments and shows the experiment results using various evaluation metrics. Finally, in Sect. 5, conclude this work with future directions.

2 Related work

In recent times, there have been significant efforts to ensure the safety and security of systems, sensors, and devices that are based on the IIoT and IoT. These efforts include creating secure detection systems and developing strategies to detect and prevent malicious activities in IIoT and IoT applications. Also, as the amount of data sent by IIoT applications grows, it is more important than ever to have effective Intrusion detection systems (IDS). Machine learning (ML) and DL, which are a part of AI that utilizes neural networks, have gained significant attention in cyber security, and many researchers have investigated their potential in detecting intrusions in IoT and IIoT networks.

To recognize various IoT infrastructure attacks, authors in [6], proposed an IDS that utilizes ML algorithms. Their suggested approach includes decreasing the features using the principal component algorithm (PCA) and linear discriminate analysis (LDA) before classifying different attacks using k-NN (k-nearest neighbor) and naïve Bayes methods. A hybrid CNN-LSTM (Convolutional neural network-LSTM) model is introduced by the authors in [7], for identifying IoT cyberattacks. The CICIDS2017 dataset is used to assess the model's performance and detect attacks. Their model makes use of features from the application layer. The accuracy of the proposed technique is 97.16%. In [8], their study proposed a hybrid CNN-LSTM-based neural network model to identify different attacks in network traffic at the edge of the IIoT. The suggested approach exclusively makes use of features that enhance privacy at the transport and network layers. Results reveal that, in a dataset containing IIoT traffic, the proposed model achieves an average accuracy of 97.85% in categorizing traffic as benign or malicious and an average accuracy of 97.14% in identifying 15 particular attacks. In [9], the authors suggested an intelligent network model for detecting cyber-attacks in the context of IoT based on the multi-class categorization called inception time, which is an ensemble of DCNN (Deep Convolutional neural networks) models. The Edge-IIoTset dataset was used to evaluate the proposed model. Many studies have been conducted on intrusion detection systems for the Internet of Things, as mentioned in [10, 11]. The datasets employed in

these experiments, however, are not representative of real-world IoT events and so are unable to replicate reality. Also, the majority of datasets used in the literature have been pre-processed, which means that the features have been altered in a way that does not exactly match the features from the network data frame. Because of this, classification requires more pre-processing stages, which makes real-time implementation challenging. The authors in [12], created a test environment that involved multiple layers such as cloud, NFV (Network functions virtualization), edge, and SDN (Software-defined network) along with various IoT and IIoT devices. They generated a large dataset by subjecting these devices to normal as well as attack traffic. The dataset was used to evaluate ML models with two approaches: centralized and federated learning. The authors used a Decision tree (DT), Random Forest, SVM (Support vector machine), k-NN, and DNN (Deep neural network) for centralized learning, and the same DNN for federated learning. However, the centralized learning approach could only analyze a limited portion of the traffic. Although the accuracy of the models was good, with above 94% for multiclass and 99.99% for binary classification, the analysis only covered 75% of the entire dataset. The authors in [13], proposed a detection method for the healthcare industry that utilized an optimized LightGBM (Light Gradient Boosting machine) and a BERT-based transformer model. The performance of the models was evaluated on three datasets besides the Edge-IIoTset, which was also used in a previous study [9]. However, the authors pointed out that the Edge-IIoTset may not be diverse enough or representative of a real-world testbed. The proposed method achieved a score of over 99% using the AUC (Area under the curve) metric for classifying the four datasets. Additionally, the LightGBM model achieved a perfect accuracy of 100% for binary classification and an average precision, recall, and F1-score of 92%, 88%, and 89%, respectively, for 14 types of attacks other than the normal class in 15 multiclass classifications. The authors of [14], investigated using different datasets. It is challenging to separate data from the application layer since a large number of them have already undergone flow-preprocessing. With the exception of the Edge-IIoTset dataset, which retains information even when application layer features are removed, most datasets contain IIoT traffic. For instance, the TCP layer can only be used to analyze three features after the removal of the MQTT set features. Similar to this, the TCP characteristics in MQTTIOT-IDS are control flag features. In [5], authors have presented an enhanced Intrusion Detection system that combines GWO (Grey wolf optimizer) and LSTM for improved accuracy in identifying cyber-attacks. They evaluate the proposed scheme using the datasets UNSW-NB15 and NSL KDD and compare it with existing strategies. The results demonstrate significant performance improvements, achieving a 96.1% accuracy for NSL-KDD and 97.4% accuracy for UNSW-NB15 datasets. The results indicate its effectiveness in enhancing network security. In [18], authors introduced a new classification algorithm based on Relief-F feature weighting and distance measures for intrusion detection. The performance of this algorithm is compared to well-known ML algorithms such as Naïve Bayes, DT, and SVM in terms of key metrics including Detection Rate, Accuracy, FAR, F-Score, and MCC. To validate the classification algorithm's effectiveness, it is tested using KDDcup99 and Kyoto 2006+ datasets. Results demonstrate its superiority over established algorithms in terms of detection performance and execution time, while also exploring its parallelization capabilities. In [19], authors show the realm of modern cybersecurity; traditional IDS struggle to effectively identify sophisticated cyberattacks characterized by unpredictable patterns. Keeping pace with the exponential growth of network data and features is a significant challenge for existing ML-based detection methods in the field of information technology. To address this issue, they used the DCNN model. Traditional CNN are limited by their parameter constraints and vulnerability to local optimization. This paper introduces a DCNN model designed to enhance attack detection capabilities and evaluates its performance in an SDN environment. Additionally, the model is trained on the CIC-DDoS2019 and CIC-IDS2017 datasets. The results showcase the superiority of the proposed DCNN model over many recent attack detection methods, achieving an impressive 99.99% accuracy rate with an exceptionally low loss rate of 0.0016. In [20], the authors introduce a novel approach known as RFOFS-ODLID (Red Fox Optimizer-based Feature Selection with Optimal Deep Learning-based Intrusion Detection) to enhance network security. The proposed method is designed to identify and classify intrusions, ultimately contributing to network security. Feature selection is performed using the RFOFS-ODLID technique to determine the optimal feature set. To identify and classify intrusion RFOFS-ODLID method utilizes the GRU technique with Adamax optimizer. The experimental findings demonstrate that the proposed technique outperforms existing methods, highlighting its effectiveness in enhancing network security and intrusion detection.

From the above discussion, it is clear that researchers have been working on ways to detect and categorize malicious activities or different types of threats and attacks. Although researchers have used several datasets with different sample sizes for training and testing, these studies have often been constrained by a limited selection of datasets and categories of cyber-attacks. In contrast, in this study, we propose a DL-based system for detecting and classifying cyber threats in 5G-enabled IIoT networks. Our system is capable of distinguishing between different classes of attacks and achieves good results on considered datasets.

3 The proposed architecture for 5G enabled cyber security threat detection on industrial IoT

This section discussed the proposed 5G threat detection DL model followed by a dense layer and classifier that is used to classify the threat. The step-by-step architectural framework for this proposed model is outlined in Algorithm 1.

Algorithm 1: Proposed threats detection system

1. Input- Read Edge-IIoTset dataset = DS
2. Output- Multiclass threats or attack classification
3. Split the DS into DS_{Train} and DS_{Test}
4. ***for*** each layer of Sk-LSTM do
5. Apply preprocessing on trainset $DS'_{Train} = DS_{Train}$
6. Build the threats detection model using Sk-LSTM DL_{model} = Train the SkLSTM model using DS'_{Train}
7. ***end for***
8. Preprocessing on testset $DS'_{Test} = DS_{Test}$
9. ***while*** True **do**
10. Detectthreattype -> DL_{model} (DS'_{Test})
11. ***if*** value = 0 then
12. Return type normal
13. ***else***
14. Return type threats
15. ***end if***
16. ***end while***

In this study, we presented a 5G-enabled Industrial IoT system. This technology can be used in an array of smart applications, such as smart agriculture, healthcare, and cities. The proposed approach captures the essential data using intelligent sensors, meters, machines, and IoT-based chips and then transmits this data via the internet through 5G infrastructure. Fifth-generation network provides low latency and fast communication links to smart devices, sensors, and systems, allowing data to be processed efficiently and sent to the cloud or edge servers. However, like traditional methods, sensors, communication links, and IoT devices are targeted by attackers [4]. The activities of attackers intercept the information generated from the IIoT and IoT devices. An attacker can take control of an insecure and susceptible device, machine, or system and use it as a launchpad for attacks or threats against other network devices, which have an impact on the machine's ability to function normally across industries. So, a smart system that can detect such attacks and restrict the machine from superfluous actions is required in this scenario. In order to detect and classify cyber-attacks from the collected data, we leverage AI and pass the information through a stacked LSTM. As an industry adopts a more frequently used IIoT-based system, it will become necessary to use an efficient system and attack prevention techniques. In Fig. 1, it can be seen that the collected data from the various devices is passed through multiple layers of LSTM that can help to classify the cyber-attack, and information is sent back to the server.

3.1 Stacked LSTM for cyber attack detection

LSTM is a type of RNN (Recurrent neural network) that is specifically designed to model sequential data. RNNs are able to capture complex patterns in sequential data by using feedback connections, which allows information to be passed from one-time step to the next. However, RNNs can have difficulty learning long-term dependencies in time series data due to issues with the gradient vanishing or exploding.

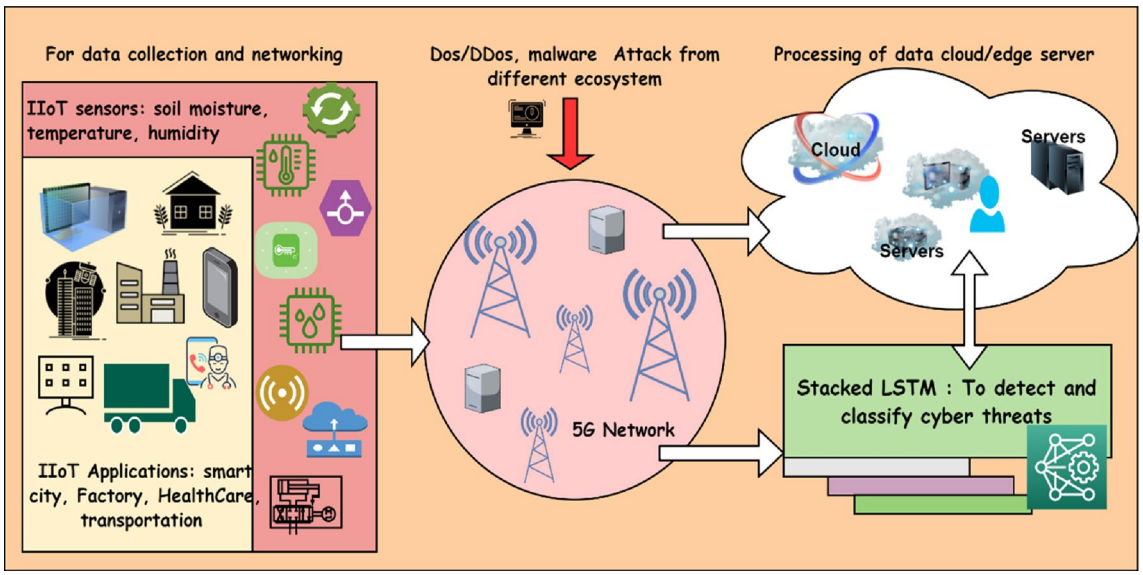

Fig. 1 Architecture for a 5G enabled IIoT cyber security threat detection system

LSTM's architecture is a solution to the RNN's gradient problem, where the network struggles to learn long-term dependencies in sequential data. Long-term dependencies can be represented by the memory cell in an LSTM. The memory cell has four gates, which control how the memory units interact with one another. The output gate determines whether other memory cells' statuses can be modified, whereas the input gate determines whether to modify the status of the memory cell based on the input signal. The forget gate has the option of remembering or forgetting its prior status. At each time step, a series of equations that are dependent on the specific LSTM structure is used to update.

the hidden layer of LSTM memory cells [15].

Figure 2 represents the LSTM for cyber threat detection. In this study, we have defined a sequential model with multiple LSTMs and dense layers for detecting the normal and attack types on the Edge-IIoTset dataset. We define a stacked LSTM model with two LSTM layers. The first and second LSTM layers have 128 and 64 units, respectively. The first LSTM layer returns a sequence of outputs rather than a single output, and the second LSTM layer takes the output sequence from the first LSTM layer as input. The next four dense layers have 512, 256, 128, and 64 units, respectively, with ReLU activation functions. The final dense layer with the SoftMax activation function is the output for multiclass classification. We then compile the model with the Adam optimizer and categorical cross-entropy loss function. We also specify the accuracy metric to monitor during the training. Finally, we train the model for 15 epochs with a batch size of 128 and a learning rate of 0.001 and validate the model on a validation set. The main advantages of SkLSTM are that, by stacking LSTM layers, a model can learn encoded feature characteristics from multiple perspectives at each time step, and its parameter distribution strategy spreads the model's parameters across the model space without increasing memory capacity, leading to faster convergence and more efficient optimization of nonlinear operations on raw data.

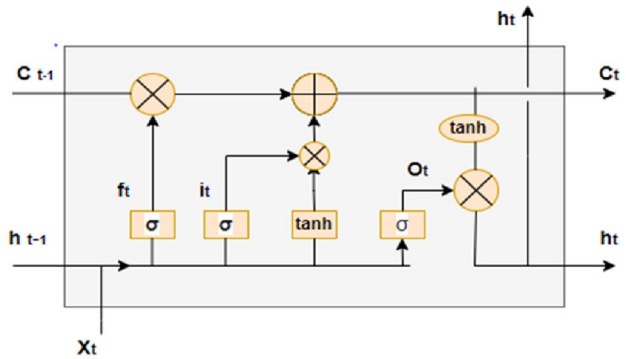

Fig. 2 LSTM for cyber threat detection

$$f_t = \sigma(w_{hf} h_{t-1} + w_{xf} * x_t + w_{cf} c_{t-1} + b_f) \quad (1)$$

$$i_t = \sigma(w_{hi} h_{t-1} + w_{xi} * x_t + w_{ci} c_{t-1} + b_i) \quad (2)$$

$$o_t = \sigma(w_{ho} h_{t-1} + w_{xo} * x_t + w_{co} c_t + b_o) \quad (3)$$

$$c_t = f_t c_{t-1} + i_t \tanh(w_{xc} * x_t + w_{hc} * h_{t-1} + b_c) \quad (4)$$

$$h_t = o_t * \tanh(c_t) \quad (5)$$

In Eqs. (1)–(5) i_t, f_t, o_t, c_t denoted by input, forget, and output gate and cell state gates at the t time respectively. The tanh and σ are tangent functions and sigmoid functions respectively. w is the weight of respective gate neurons, x_t is the current input and b_x is a bias of the respective gate. h_{t-1} and c_{t-1} are the hidden and cell state at time step $t-1$ respectively [15].

4 Experiment result and discussion

In this section, we discussed the experimental setup followed by the description of the dataset, data preprocessing, and performance metrics. The Python language is used to conduct the experiments. SkLSTM model is implemented using the Keras API of tensor flow. The deep learning model performance is tested using the publicly available Edge-IIoTset data set. Experiments are performed on an Intel® Xeon® CPU E3-1240v6 operating at 3.70 GHz with 16 GB RAM.

4.1 Edge-IIoT dataset description

This dataset related to cyber security in the IoT and IIoT domains encompasses key IoT attributes and diverse network traffic. The data are generated from different IoT and IIoT devices such as heart rate sensors, pH sensor meters, etc. This dataset contains fourteen attacks related to IoT and IIoT environments. Such attacks include malware, MITM, DoS and DDoS, injection attacks, and information-gathering attacks. This dataset contains 61 features, including a normal vector and 14 types of attacks [12].

4.2 Data preprocessing

During the data preprocessing steps, the complete dataset is used for evaluation. Some predefined steps are followed. It includes feature mapping, which converts categorical data into numeric data using label encoding, and drops the missing and duplicate values. The standard scaler is used to scale

IIoT traffic to a specific scale. Then, the data is split into two parts, with 70% being used for training and 30% for testing.

4.3 Description of performance measures

The performance measure is used to evaluate the performance of the efficacy model. These measures include DR′ (detection rate), also known as recall, accuracy (Acc), F1-Score, and precision (PR′). The numerical Eqs. (6)–(9) used for calculating the Acc, PR′, DR′, and F1-Score are given below. Various parameters are used for computing these values, where TNe, TPs, FNe, and FPs represent True Negative, True Positive, False Negative, and False Positive, respectively [8]. The performance measures are calculated using the mentioned parameters and are given below [15].

$$Acc = \frac{TPs + TNe}{TPs + TNe + FPs + FNe} \tag{6}$$

$$PR\prime = \frac{TPs}{TPs + FPs} \tag{7}$$

$$DR\prime = \frac{TPs}{TPs + FNe} \tag{8}$$

$$F1 - Score = \frac{2 * PR' * DR'}{PR' + DR'} \tag{9}$$

4.4 Result and discussion

For the edge-IIoTset dataset, the cyber threat detection system contains multiple classes by adding normal and attack traffic instances. The dimension of the training and testing dataset is mentioned in Table 1. The class-wise prediction results obtained from the considered dataset are represented in Table 2. SkLSTM outperformed Normal (0), ICMP DDoS (2), MITM (6), UDP flood DDoS (4), and TCP SYN Flood DDoS (3) in terms of precision, detection rate, and F1-score. Table 2 presents the model's average PR′, DR′, and F1-score, which are 99.43%, 98%, and 98.46%, respectively. Figure 3 shows the training versus validation loss, and training vs validation accuracy of SkLSTM using the Edge-IIoTset dataset, respectively. 5G-enabled SkLSTM has achieved 98.30% validation accuracy, 3.7% validation loss, 99.43% precision, 98% detection rate, and 98.46% F1-Score. The performance of the proposed system is evaluated using the SkLSTM DL-based technique. The proposed 5G-enabled SkLSTM is evaluated using the Edge-IIoT dataset. The preprocessing steps are discussed in Sect. 4. The proposed system performance was evaluated using training accuracy vs. validation Loss, class-wise prediction score, and confusion matrix. The SkLSTM configuration is discussed above.

Table 1 Statistics for a total number of observations selected for both testing and training

Class label	Total	Train	Test
UDP flood DDoS (4)	121,567	85,119	36,448
Normal (7)	1,380,858	966,804	414,054
ICMP flood DDoS (2)	67,939	47,475	20,464
SQL Injection (11)	50,826	35,675	15,151
MITM (6)	358	251	107
OS fingerprinting (5)	853	593	260
Ransomware (10)	9689	6795	2894
Cross-site scripting (XSS) (14)	25,557	10,599	14,958
Backdoor (0)	24,026	16,685	7341
Port scanning (9)	19,983	13,914	6069
Upload (12)	36,915	25,662	11,253
HTTP flood DDoS (1)	49,203	34,522	14,681
Vulnerability scanning (13)	46,321	35,068	11,253
TCP SYN flood DDoS (3)	50,062	34,954	15,108
Password cracking (Pwd) (8)	49,933	34,996	14,937

Table 2 Class wise prediction results obtained from the Edge-IIotset dataset

Attack categories	PR′	DR′	F1-score
Backdoor attack (0)	0.99	0.96	0.98
HTTP flood DDoS (1)	0.96	0.92	0.94
ICMP flood DDoS (2)	1.00	1.00	1.00
TCP SYN flood DDoS (3)	1.00	1.00	1.00
UDP flood DDoS (4)	1.00	1.00	1.00
OS Fingerprinting (5)	1.00	0.69	0.80
MITM (6)	1.00	1.00	1.00
Normal (7)	1.00	1.00	1.00
Password cracking (8)	0.99	0.70	0.82
Port Scanning (9)	0.95	0.98	0.96
Ransomware (10)	0.96	1.00	0.98
SQL Injection (11)	0.98	0.74	0.84
Upload attack (12)	0.92	0.72	0.81
Vulnerability scanning (13)	0.98	0.95	0.97
Cross-site Scripting (XSS) (14)	0.86	0.92	0.89
Avg (%)	99.43	98.00	98.46

Table 3 shows the performance comparison with some of the existing work. In order to assess the performance of models, we have employed a confusion matrix to provide a visual representation of how well our predictive model is performing and observe confusion between different labels. Each row in the matrix represents the true labels, while columns represent the predicted labels. The elements along the main diagonal of the matrix indicate correct prediction, while the value outside the diagonal indicates a misclassified prediction. Figure 4, shows the confusion matrix for classification

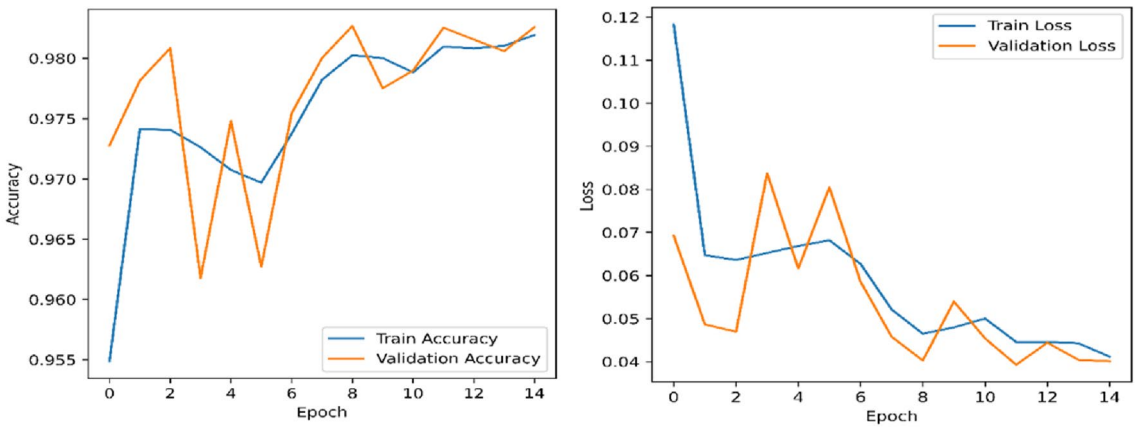

Fig. 3 Training and validation Acc vs training and validation loss obtained from the DL-SkLSTM

Table 3 Performance comparison with existing threat detection methods

Authors	Model	Year	Class	Acc (%)
Ferrag et al. [12]	DNN	2022	Multiclass	96.01
Ferrag et al. [12]	RF	2022	Multiclass	80.83
Ferrag et al. [12]	SVM	2022	Multiclass	77.61
Tareq et al. [9]	Inception time	2022	Multiclass	94.94
Erik et al. [8]	CNN-LSTM	2022	Multiclass	97.14
Our proposed	Stacked-LSTM	2023	Multiclass	98.30

problems involving 15 distinct classes. A comparison of the proposed SkLSTM in terms of the performance metrics against random forest and Gated recurrent unit (GRU) can be observed in Fig. 5.

5 Conclusion

In the proposed study, a 5G-enabled system that uses a DL approach to find and classify different types of cyber-attacks on the IIoT is introduced. The detection system uses the DL approach, i.e., stacked LSTM then evaluated on the Edge-IIoTset dataset. The experiment results were compared to the state-of-the-art techniques; the results showed

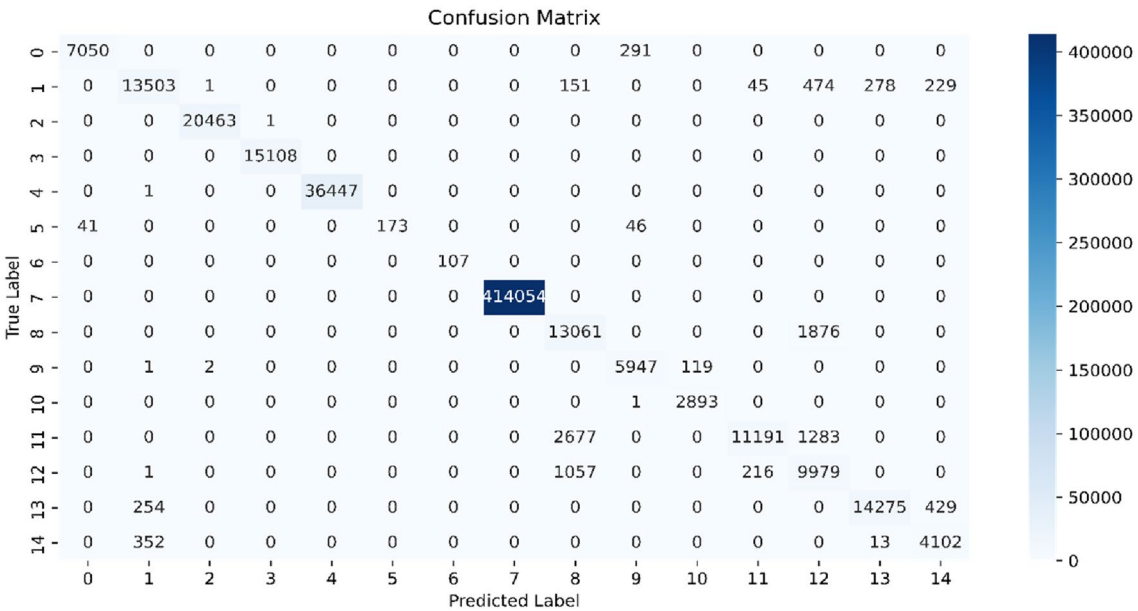

Fig. 4 Confusion matrix obtained from the DL-SkLSTM

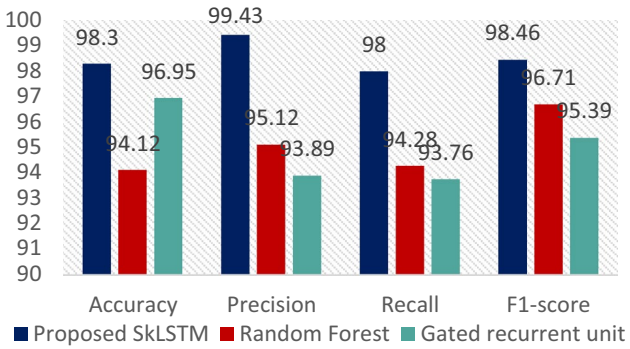

Fig. 5 Performance comparison against random forest and GRU

that the proposed system's detection accuracy is improved. The detection system achieved 98.30% accuracy and a 98% detection rate on the publicly available dataset. We maintain the perspective that there remains a substantial need for further research in the realm of 5G-enabled IoT to achieve an improved detection rate as the industry continues to advance. Our future endeavors will focus on the exploration of DL techniques and rigorous testing of the proposed system using other realistic datasets related to IIoT and IoT. Furthermore, we intend to explore the integration of blockchain.

Declarations

Conflict of interest The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Ahmad M, Ahmed I, Jeon G (2021) An IoT-enabled real-time overhead view person detection system based on Cascade-RCNN and transfer learning. J Real Time Image Proc 18:1129–1139
2. Moustafa N et al (2020) Federated TON_IoT Windows datasets for evaluating AI-based security applications. In: 2020 IEEE 19th international conference on trust, security, and privacy in computing and communications (TrustCom). IEEE
3. The internet of things 2020: here's what over 400 IoT decision-makers say about the future of enterprise connectivity and how iot companies can use it to grow revenue. https://www.businessinsider.com/internet-of-thingsreport?IR=T, https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307. Accessed 3 Jan 2022
4. Ahmed I et al (2022) A multilayer deep learning approach for malware classification in 5G-enabled IIoT. IEEE Trans Ind Inform 19(2):1495–1503
5. Karthic S, Manoj Kumar S, Senthil Prakash PN (2022) Grey wolf-based feature reduction for intrusion detection in WSN using LSTM. Int J Inf Technol 14(7):3719–3724
6. Pajouh HH et al (2016) A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks. IEEE Trans Emerg Top Comput 7(2):314–323
7. Roopak M, Tian GY, Chambers J (2019) Deep learning models for cyber security in IoT networks. In: 2019 IEEE 9th annual computing and communication workshop and conference (CCWC). IEEE
8. de Elias EM et al (2022) A hybrid CNN-LSTM model for IIoT edge privacy-aware intrusion detection. In: 2022 IEEE Latin-American conference on communications (LATINCOM). IEEE
9. Tareq I et al (2022) Analysis of ToN-IoT, UNW-NB15, and edge-IIoT datasets using DL in cybersecurity for IoT. Appl Sci 12(19):9572
10. Alsamiri J, Alsubhi K (2019) Internet of things cyber-attack detection using machine learning. Int J Adv Comput Sci Appl. https://doi.org/10.14569/IJACSA.2019.0101280
11. Al-Taleb N, Saqib NA (2022) Towards a hybrid machine learning model for intelligent cyber threat identification in smart city environments. Appl Sci 12(4):1863
12. Ferrag MA et al (2022) Edge-IIoTset: a new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. IEEE Access 10:40281–40306
13. Ghourabi A (2022) A security model based on lightGBM and transformer to protect healthcare systems from cyberattacks. IEEE Access 10:48890–48903
14. Ullah I, Mahmoud QH (2022) An anomaly detection model for IoT networks based on flow and flag features using a feed-forward neural network. In: 2022 IEEE 19th annual consumer communications & networking conference (CCNC). IEEE
15. Kumar R et al (2021) SP2F: a secured privacy-preserving framework for smart agricultural unmanned aerial vehicles. Comput Netw 187:107819
16. Shahin M et al (2022) A novel fully convolutional neural network approach for detection and classification of attacks on industrial IoT devices in smart manufacturing systems. Int J Adv Manuf Technol 123:2017–2029
17. Khacha A et al (2022) Hybrid deep learning-based intrusion detection system for industrial internet of things. In: 2022 5th International symposium on informatics and its applications (ISIA). IEEE
18. Ashok Kumar D, Venugopalan SR (2019) A design of a parallel network anomaly detection algorithm based on classification. Int J Inf Technol 14:2079–2092
19. Hnamte V, Hussain J (2023) An efficient DDoS attack detection mechanism in SDN environment. Int J Inf Technol. https://doi.org/10.21203/rs.3.rs-2393388/v1
20. Sunkara S, Suresh T, Sathiyasuntharam V (2023) Red fox optimizer-based feature selection with optimal deep learning-based Intrusion detection for network security. Int J Inf Technol 15:4437–4447
21. AbdulRaheem M et al (2023) Machine learning assisted snort and zeek in detecting DDoS attacks in software-defined networking. Int J Inf Technol. https://doi.org/10.1007/s41870-023-01469-3
22. Usoh M et al (2023) A hybrid machine learning model for detecting cybersecurity threats in IoT applications. Int J Inf Technol 15(6):3359–3370

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.