STM JOURNALS

Journal of
Web Engineering & Technology
https://journals.stmjournals.com/jowet

ISSN: 2455-1880
Volume 13, Issue 1, 2026
January–April
DOI (Journal): 10.37591/JoWET

Review JoWET

Enhancing IoT Network Security with Hybrid Deep Learning Classifiers for DDoS Attack Detection

Manjusha V. Khond[1,*], Mahesh R. Sanghavi[2]

Abstract

The security and operational dependability of Internet of Things (IoT) networks are seriously threatened by the growing susceptibility to Distributed Denial of Service (DDoS) assaults brought about by their rapid expansion. The intricacy and dynamic character of these advanced attacks can provide a challenge to conventional intrusion detection systems. This study presents a novel method for strengthening IoT network security by combining Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks into a hybrid deep learning framework. The suggested CNN-LSTM approach ensures precise and effective DDoS threat detection by utilizing CNNs' advantages for feature extraction and LSTMs for temporal dependency modelling. The capacity of the model to minimize security threats is shown by the assessment findings, which indicate that it performs better than existing methods in accuracy, precision, and recall. This study highlights the strength of hybrid deep learning models as a solid solution for safeguarding IoT ecosystems against sophisticated cyber-attacks.

Keywords: Hybrid deep learning classifiers, CNN, LSTM, DDoS, IoT

INTRODUCTION

The Internet of Things (IoT) connects any device to the Internet, forming the foundation of this technology. This has led to the development of smart cities, where critical infrastructure such as energy, water resources, and traffic systems are monitored and managed online [1]. The Internet of Things (IoT), a global network assigned unique addresses, has witnessed remarkable growth in recent years. IoT devices utilize diverse communication protocols and sensor capabilities, enabling data analysis and service provision [2]. However, the rapid expansion of IoT, alongside advancements in fields such as medical systems, electric vehicles, and 5G networks, has increased exposure to cyber threats. Cyberattacks, which were initially aimed at traditional computer networks, now frequently target IoT systems, leading to risks such as Distributed Denial of Service (DDoS) attacks, spoofing, data breaches, and gateway compromises. These vulnerabilities are exacerbated by inadequate security measures and the absence of intelligent intrusion detection mechanisms. A DDoS attack, a malicious method that floods a target system with data to overwhelm its bandwidth or resources, disrupts network services and renders them inaccessible [3]. Intrusion Detection Systems (IDS) leveraging Machine Learning (ML) and Deep Learning (DL) algorithms have proven more effective than traditional techniques in identifying these threats. However, as cyberattacks become more complex, ML-based systems face challenges such as overfitting. Popular supervised ML techniques for IoT attack detection include K-Nearest Neighbor (KNN), Neural Networks (NN), and Support Vector

***Author for Correspondence**
Manjusha V. Khond
E-mail: manjushakhond@gmail.com

[1]Research Scholar, Computer Engineering, Mumbai Educational Trust, Institute of Engineering, Bhujbal Knowledge City, Nashik, Maharashtra, India
[2]Professor & Vice-Principal, Computer Engineering, S.N.J.B. Engineering College, Chandwad, Maharashtra 423101, India

Received Date: June 12, 2025
Accepted Date: September 05, 2025
Published Date: November 17, 2025

Citation: Manjusha V. Khond, Mahesh R. Sanghavi. Enhancing IoT Network Security with Hybrid Deep Learning Classifiers for DDoS Attack Detection. Journal of Web Engineering & Technology. 2026; 13(1): 23–33p.

Machines (SVM) [4]. Recent studies have demonstrated the exceptional efficiency of DL, particularly in detecting cyberattacks within smart city environments. Hybrid DL models have shown superior performance, achieving high accuracy rates in detecting and mitigating threats [1].

This research focuses on analyzing hybrid DL methods through a review of existing literature. The survey highlights that most current research emphasizes detecting IoT attackers using DL techniques. Key aspects considered in the analysis include performance measures, methodology, and the results considered with IoT security.

The following is the study's structure: The next Section gives an overview of current deep learning techniques for attack detection. The hybrid CNN-LSTM model for identifying DDoS assaults in IoT networks is presented in the section after that. The difficulties and research gaps found throughout the study are highlighted in the section thereafter. Then the findings and the conclusions are presented in the last sections.

RELEVANT LITERATURE

Nowadays, hybrid deep learning (DL) models have become effective tools for identifying and addressing security threats [5–7], such as botnet attacks and distributed denial of service (DDoS) in Internet of Things (IoT) networks. These models combine several deep learning (DL) and machine learning (ML) techniques to improve attack detection systems' scalability, accuracy, and efficiency. This review presents a summary of recent studies that have explored hybrid DL models for attack detection in IoT systems.

Elsaeidy *et al*. suggested a hybrid model by combining the Boltzmann Machine and deep Convolutional Neural Networks (CNN) to detect both DDoS and replay attacks. The hybridized model addresses the limitations of traditional methods, such as insufficient feature extraction and the complexity of probabilistic distributions in the data. By generating data related to these attacks, the model demonstrated improved performance in attack detection [1].

Sahu *et al*. presented a hybrid model that combines CNN and Long Short-Term Memory (LSTM) classifiers in order to detect malicious attacks. The model accurately extracts features and classifies attacks, balancing the computational overhead with high detection accuracy. The hybrid approach shows promise in simplifying security modeling in IoT environments [8].

Javeed *et al*. combined CUDA-bidirectional LSTM (Cu-BiLSTM and CUDA-deep Neural Network (Cu-DNN gated recurrent unit (GRU) for efficient attack detection. This model outperforms traditional methods by providing fast detection with high accuracy, reducing the testing time to only a few seconds [2].

Najafimehr *et al*. employed a hybridization of density-based clustering with noise algorithms and Principal Component Analysis (PCA) for detecting the attacks. This approach splits normal data from anomalous traffic by utilizing unsupervised and supervised algorithms, improving the accuracy of attack detection [9].

Ullah *et al*. developed a hybrid model to detect malicious attacks in IoT networks by combining LSTM and GRU. The model achieves high detection accuracy, and its performance can be enhanced by integrating additional layers to overcome the model's initial limitations [3].

Alghazzawi *et al*. demonstrated a hybrid model combining CNN and BiLSTM classifiers, focusing on IoT networks' feature selection. Although this model achieves effective attack detection,

it faces limitations due to the use of single data sources and statistical methods for feature selection [10].

Alzahrani and bamhdi introduced a CNN-LSTM hybrid model for detecting attacks in IoT devices, focusing on common attacks in IoT security systems. Their model demonstrated optimal performance, offering valuable insights into DL networks' capabilities for attack detection [11].

Sagu *et al*. proposed an optimally tuned Deep Belief Network (DBN) hybridized with firefly and grey wolf algorithms. The model enhances classification accuracy through optimal tuning of the activation function, but requires further improvement due to its time-consuming and complex nature [12].

Xinlong and zhibin presented a hybrid DL method utilizing hierarchical memory with LSTM to detect malicious web attacks. This unsupervised learning model does not require labeled data, simplifying the detection process [13].

Cil *et al*. applied Deep Neural Networks (DNN) for detecting and classifying attackers in network signals, demonstrating high precision in detecting DDoS attacks. Their work emphasizes the effectiveness of hybrid DL methods in real-time data attack detection [14].

Alzahrani explored six Machine Learning algorithms, including K-Nearest Neighbor (KNN), Support Vector Machine (SVM), Naive Bayes (NB), Decision Tree (DT), Random Forest (RF), and Logistic Regression (LR) for intrusion detection in IoT networks. However, they noted the challenges in obtaining publicly available IoT traffic datasets for training and evaluation [15].

Popoola *et al*. tackle the issue of class imbalance in attack detection by hybridizing SMOTE (Synthetic Minority Over-sampling Technique) with Deep Recurrent Neural Networks (DRNN). This approach improved hierarchical feature representation but was still affected by imbalanced data in training samples [16].

Niraja and srinivasa rao applied a deep autoencoder for detecting malicious attacks. Their method showed significant improvement over traditional autoencoders in terms of classification accuracy and attack detection, emphasizing the power of deep learning in cybersecurity [17].

Islam *et al*. used ML techniques such as SVM, KNN, and RF for classifying DDoS attacks. The SVM classifier played a key role in detecting robust attacks, but the model's reliance on supervised learning and offline datasets limited its application to real-time systems [4].

Lakshmi narayanan *et al*. proposed a Naive Bayes (NB) classifier to detect DDoS attacks and evaluate the round-trip time in wireless networks. However, they acknowledged the need for further improvements, particularly through encryption algorithms for better security [18].

Al-Taleb and saqib introduced a hybrid CNN and quasi-Recurrent Neural Network (QRNN) model to improve attack classification and minimize false predictions. Despite improvements in feature extraction, the model faced challenges due to security and privacy concerns when applied to real-time data in smart cities [19].

Wazzan *et al*. focused on botnet attack detection in IoT by combining CNN and LSTM models. Although their approach showed high accuracy in early-stage attack classification, overfitting emerged as a challenge due to the lack of subsampling in the training process [20].

Ahuja *et al*. proposed a hybrid model combining SVM with RF classifiers for DDoS attack detection. Their approach achieved high classification accuracy and minimized false predictions, although the computational intensity of the model was a concern [21].

Mohmand *et al*. used hybrid classifiers, including RF and eXtreme Gradient Boosting (XG Boost), to predict and classify DDoS attacks. The absence of labeled datasets, however, limited the model's potential for better performance [22].

Alkahtani and Aldhyani hybridized CNN with LSTM for botnet attack prediction, enhancing IoT network security by detecting undetermined attack patterns. Their model proved effective in mitigating DDoS attacks but required further optimization to handle the IoT network's complexity [23].

Pokhrel *et al*. proposed the K-Nearest Neighbor (KNN) classifier to detect botnet attacks in distributed communication systems. The use of SMOTE alongside the KNN classifier played a significant role in ensuring reliable attack detection performance [24].

A survey by Abdulrahman and Singh reviewed DL techniques for detecting DDoS attacks in Internet of Things networks, highlighting the benefits of hybrid models, like CNN-LSTM, over conventional techniques. The survey also discussed challenges such as overfitting and scalability issues [25].

Thangasamy *et al*. introduced a hybrid DL framework combining CNN and Gated Recurrent Units (GRU) for real-time DDoS attack detection. This model demonstrates high performance related to precision, recall, and F1-score using benchmark datasets [26].

Ullah *et al.* suggested a hybrid CNN-LSTM model optimized for IoT systems, achieving high detection accuracy while addressing the resource constraints inherent in IoT devices [27].

Mousa and Abdullah explored an autoencoder-based intrusion detection system for anomaly-based DDoS attack detection, using datasets such as CICIDS2017 and NSL-KDD to evaluate the performance of the model [28].

Sadhwani *et al*. noted that manual hyperparameter tuning in deep learning models is time-consuming and may not yield optimal results, suggesting the use of AutoML techniques for more efficient model optimization in future research [29].

In the studies by Maguluri *et al*. and Rathod *et al.*, deep learning techniques and IoT issues are discussed [30, 31].

SYSTEM MODEL FOR DDoS ATTACK DETECTION

Proposed Model

Using the UNSW_2018_IoT_Botnet dataset, the following procedures are needed to build a CNN-LSTM model that can detect DDoS attacks in an IoT network:

Understanding the Dataset

A comprehensive dataset for identifying botnet attacks on IoT networks is UNSW_2018_IoT_Botnet. It was generated by simulating various botnet attacks targeting IoT devices, reflecting realistic network traffic patterns in an IoT environment. The dataset contains a

wide range of features that represent both normal and malicious activities, including packet-level details, flow statistics, and protocol-level information. It includes labeled instances of different attack types, such as DDoS, DoS, and scanning attacks, and offers an important tool for developing and evaluating machine learning models in cybersecurity applications.

Data Preprocessing

Performance of the CNN-LSTM model depends mainly on data preprocessing, which includes:

- *Data cleaning:* Remove or handle missing values, if any.
- *Normalization:* The numerical features are normalized to the scale of all the incoming data.
- *Encoding categorical features:* Convert categorical characteristics into numerical values by applying label encoding or one-hot encoding.
- *Sequence generation:* For the LSTM part, generate sequences of network traffic data. For example, use a window size of n to create sequences of n consecutive data points.
- *Train-Test split:* Splitting the information for test, validation, and training sets.

Model Architecture: CNN-LSTM

The CNN-LSTM model combines LSTM networks for sequence prediction with CNN for feature extraction:

- *Input Layer:* Takes a sequence of network traffic features.

CNN Layers

- *1D Convolutional layer:* Apply convolution over the sequence to capture local dependencies in the network traffic.
- *Pooling layer:* To reduce spatial dimensions while maintaining the most important information, use maximum pooling.

LSTM Layers

- *LSTM Layer:* Handles the processed features from the CNN, capturing the temporal dependencies in the sequences.
- *Fully connected layers:* Following the LSTM layer, a fully connected (dense) layer aggregates extracted features for classification.
- *Output layer:* Employs a sigmoid activation function for binary classification, while a dense layer with a Softmax activation function is utilized for multi-class classification.

Model Training

- *Assemble the model:* Select a suitable optimization algorithm, e.g., Adam; an optimization function that is appropriate, e.g., categorical cross-entropy for multi-class or binary cross-entropy for binary; and describe the evaluation metrics (e.g., recall, accuracy, precision).
- *Fine-tune the model:* To prevent overfitting, train the model on the training dataset and use early stopping with respect to validation loss.

Evaluation

Once the training is completed, the model performance can be evaluated with the test data:

- *Accuracy:* The ratio of accurately forecasted results to all observations seen.
- *Sensitivity:* The percentage of actual positive occurrences that were real positive predictions.
- *Specificity:* The fraction of actual negative cases that the model correctly classified.

RESEARCH GAPS IN THE DETECTION OF DDoS ATTACK

The various challenges associated with DL classifiers are analyzed as follows:

- The Support Vector Machine (SVM) model suffers from poor performance due to factors such as lengthy training times, high computational costs, larger requirements for testing and training data, and increased complexity [12]. Additionally, selecting an appropriate kernel function for SVM to separate data is challenging, as it often cannot be done linearly [28].
- The Random Forest (RF) model exhibits poor performance for several reasons, including its slow prediction process, unreliable attribute categorization, and a preference for smaller, more closely related groups of attributes over larger ones in the data [12].
- Deep learning models are vulnerable to adversarial attacks that can manipulate detection systems. Research should focus on making models more robust to adversarial manipulations.
- Manual hyperparameter tuning for deep learning models is time-consuming and may not yield optimal results. Auto ML techniques should be employed for efficient model optimization [29].

RESULTS AND DISCUSSION

The section interprets the outcome of the Hybrid CNN-LSTM model for the DDoS identification framework along with the performance evaluation, experimental setup, dataset description, and performance metrics, as well as the comparative evaluation and discussion.

Experimental Setup

The implementation of the CNN-LSTM attack detection model is performed in PyCharm software utilizing the Python programming language. The research harnessed the system with the specification of an i5 12th generation processor operating in a 64-bit Windows operating system. The system harnessed for experimentation contains 16 GB of RAM storage, which reduces the complexity of implementing the CNN-LSTM framework with better resources.

UNSW_2018_IoT_Botnet Dataset

This is specially designed to simulate IoT network traffic, including normal traffic and traffic from various botnet attacks, such as DDoS. It consists of several features that represent network traffic characteristics, which are employed for intrusion detection.

Features: The dataset contains features such as:

- *Flow-based features:* Like duration, protocol, packet size, flags, etc.
- *Time-based features:* Features capturing statistics over time windows.
- *Label:* Each data point is labeled as either benign or as a type of attack (e.g., DDoS, scan, etc.).

Performance Measures

Key performance indicators such as accuracy, sensitivity, and specificity are used to assess the CNN-LSTM framework's performance. The accuracy evaluates the exactness of the model in predicting the DDoS attacks on the network. The sensitivity computes the proportion of positive predicted attacks, and specificity determines the actual true negatives correctly identified by the CNN-LSTM. The proposed CNN-LSTM exhibited higher values, which shows the reliability of CNN-LSTM in DDoS detection.

Performance Evaluation

The DDoS detection efficiency of the CNN-LSTM is interpreted for various training percentages from 50 to 90 and K-Fold values from 4 to 8, respectively, as shown in Figures 1–6. The performance is analyzed for the UNSW_2018_IoT_Botnet dataset (Tables 1–6).

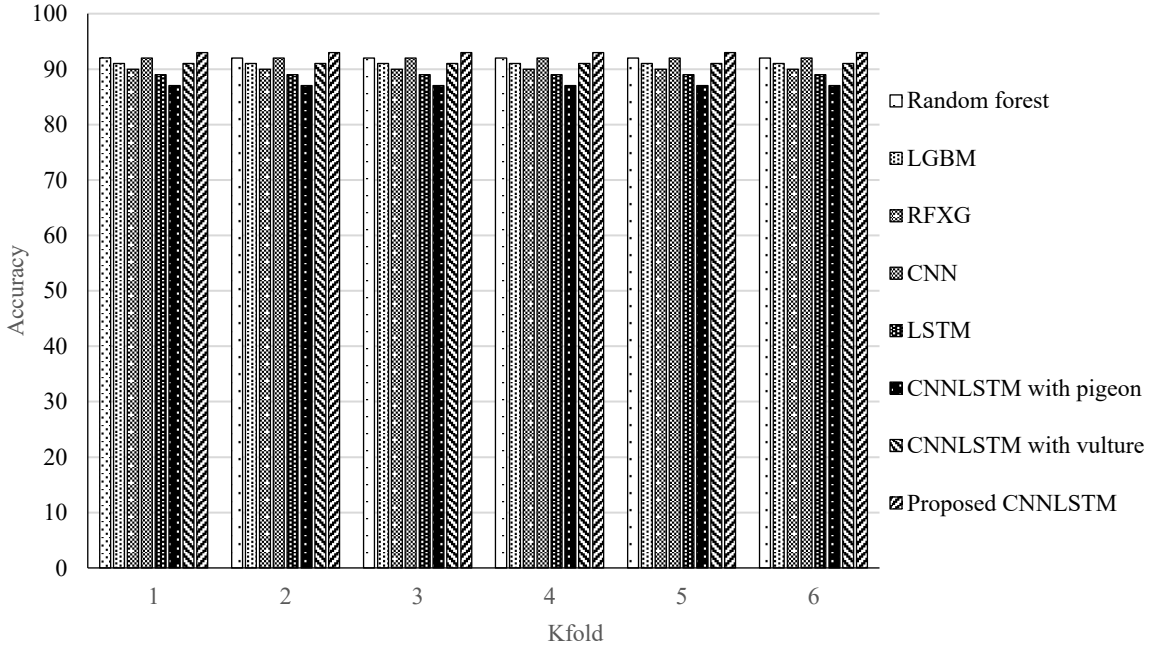

Figure 1. Accuracy vs. Kfold.

Table 1. Comparative analysis of accuracy.

.	TP_4	TP_5	TP_6	TP_7	TP_8
Random forest	89.53818	89.59015	89.653	89.5909	90.31781
LGBM	88.87111	90.57506	89.97156	90.10557	89.48289
RFXG	88.64075	89.16812	89.7011	89.33908	89.43181
CNN	89.73994	87.8957	88.79867	90.49823	89.34757
LSTM	87.53662	88.33519	90.00061	88.64759	89.23237
Proposed CNN-LSTM	91.51425	91.75765	92.14569	92.35638	92.88157

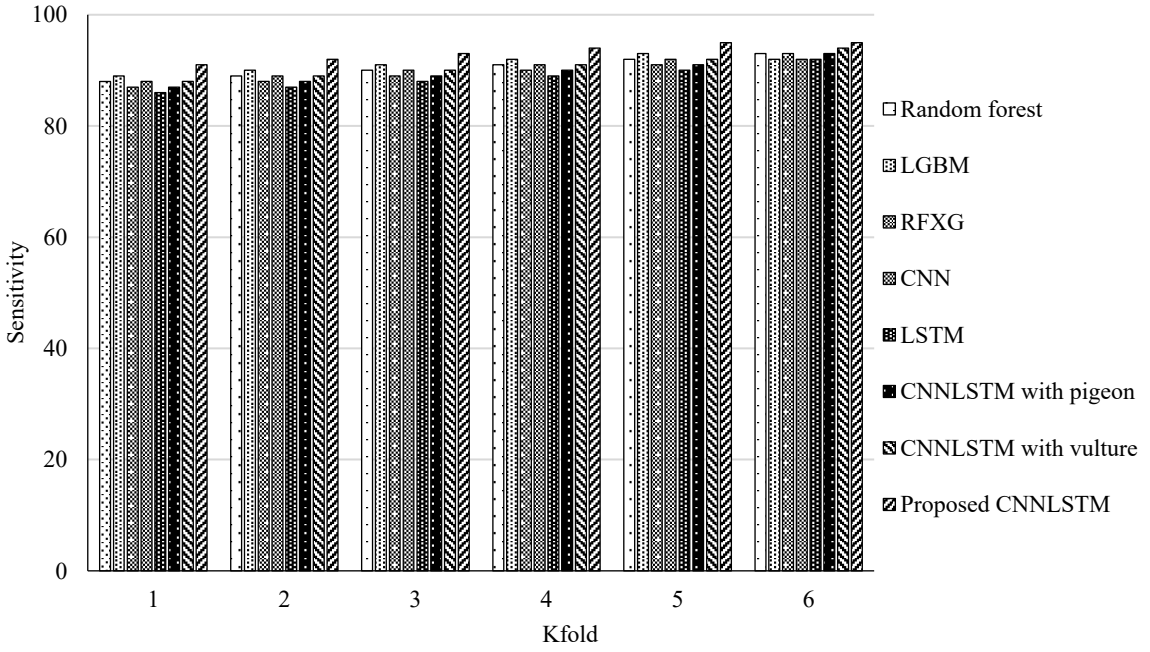

Figure 2. Sensitivity vs. Kfold.

Table 2. Comparative analysis of sensitivity.

.	TP_4	TP_5	TP_6	TP_7	TP_8
Random forest	87.80663	88.2131	89.964	90.53957	91.47699
LGBM	88.66027	89.63136	89.81323	90.22423	90.4599
RFXG	87.65095	88.79675	90.13604	90.71779	91.53289
CNN	89.51209	88.67768	89.77074	89.77356	90.04823
LSTM	86.59289	88.50506	88.94533	89.26871	90.03414
Proposed CNN-LSTM	91.6215	91.77643	92.41288	92.53671	92.78906

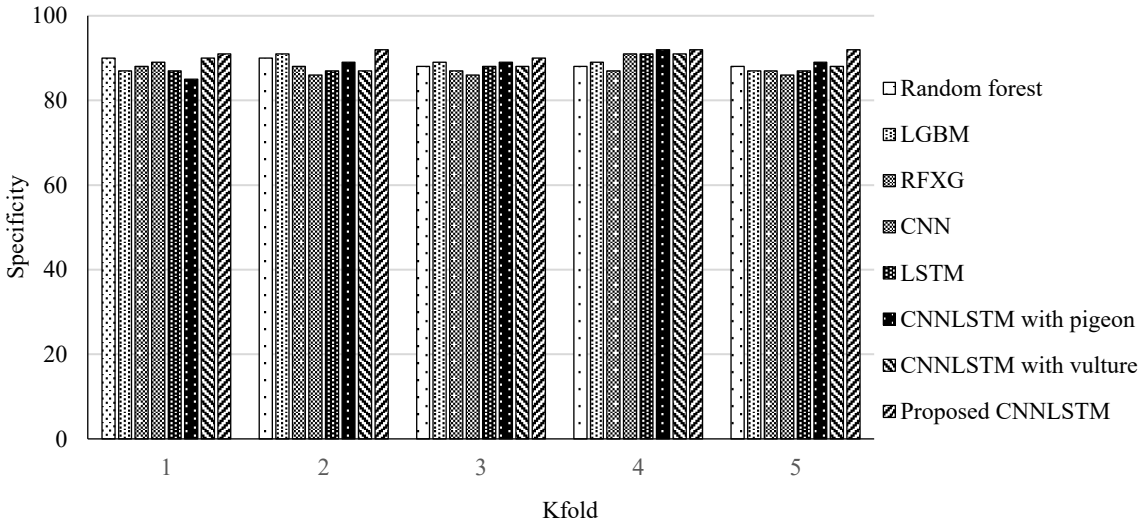

Figure 3. Specificity vs. Kfold.

Table 3. Comparative analysis of specificity.

.	TP_4	TP_5	TP_6	TP_7	TP_8
Random forest	91.26973	90.9672	89.34201	88.64223	89.15862
LGBM	89.08196	91.51876	90.12989	89.98692	88.50589
RFXG	89.63054	89.5395	89.26615	87.96037	87.33074
CNN	89.96778	87.11371	87.82659	91.2229	88.64692
LSTM	88.48036	88.16532	91.05589	88.02647	88.43059
Proposed CNNLSTM	91.40701	91.73887	91.87849	92.17604	92.97407

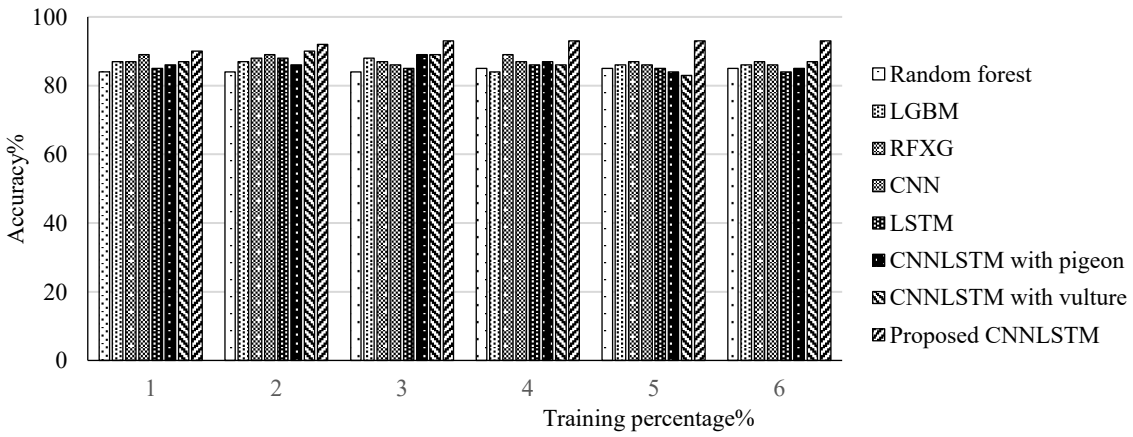

Figure 4. Accuracy vs. training percentage.

Table 4. Comparative analysis of accuracy.

.	TP_40	TP_50	TP_60	TP_70	TP_80	TP_90
Random forest	82.5	85.28226	82.56579	83.5443	88.78505	87.26415
LGBM	87.04663	87.17949	88.51351	88.7468	88.42105	92.19512
RFXG	85.64356	90.46653	86.39456	91.77378	92.92929	92.0712
CNN	89.3401	88.39458	87.04319	85.71429	91.75258	87.73585
LSTM	84.73684	84.6	89.14474	82.52427	91.57895	84.83245
PROPOSED CNN-LSTM	**92.11823**	**92.5**	**95.15571**	**95.22613**	**95.28302**	**96.08483**

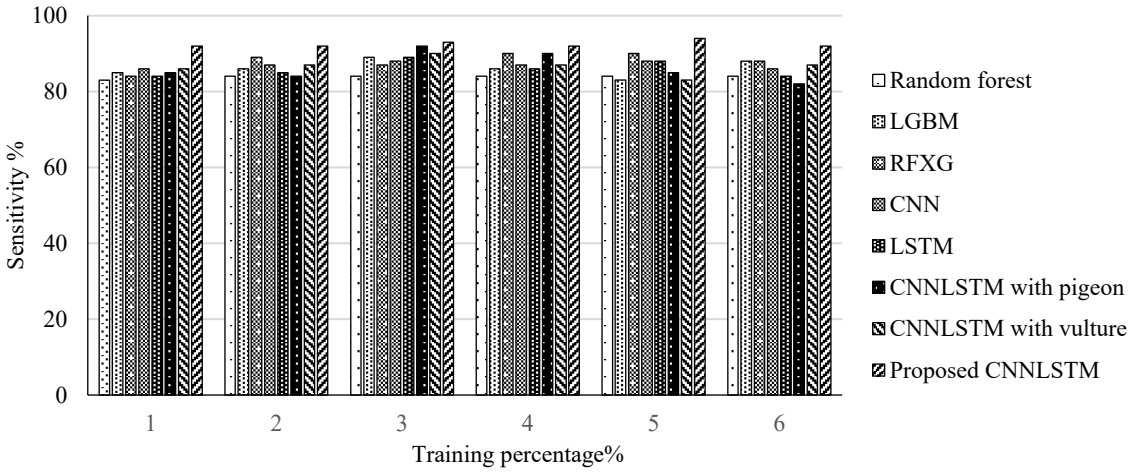

Figure 5. Sensitivity vs. training percentage.

Table 5. Comparative analysis of sensitivity.

.	TP_40	TP_50	TP_60	TP_70	TP_80	TP_90
Random forest	83.01587	84.02626	85.69779	89.11258	86.36783	86.41815
LGBM	87.03244	87.0108	89.89778	86.82623	88.34256	89.84756
RFXG	86.90462	87.39013	88.98766	91.96532	91.84178	90.75922
CNN	89.59759	89.85646	88.20245	87.56868	89.3925	90.43655
LSTM	84.06842	87.06351	86.27853	85.13006	88.70184	84.59632
PROPOSED CNN-LSTM	**91.63604**	**92.23662**	**95.10767**	**95.5078**	**95.65146**	**96.27474**

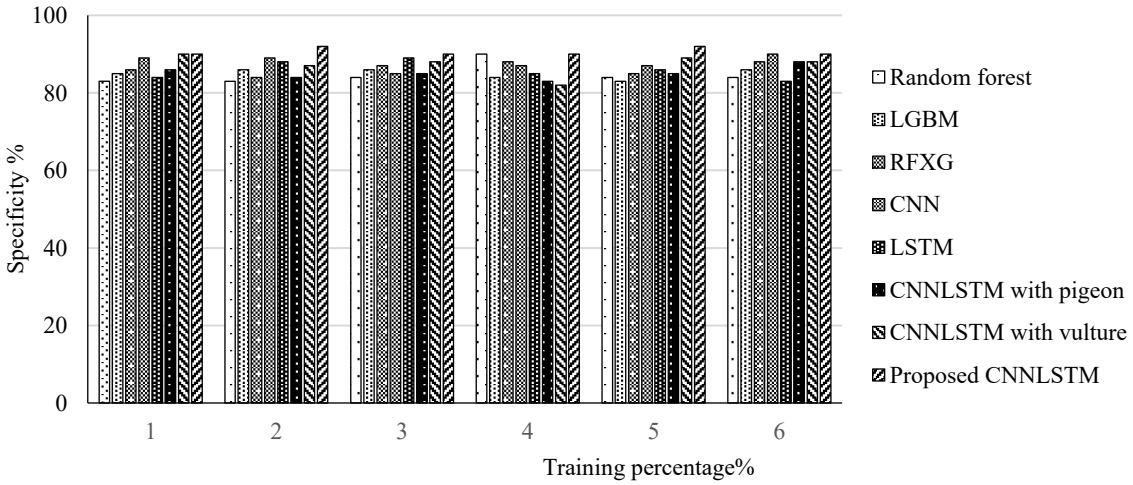

Figure 6. Specificity vs. Training percentage.

Table 6. Comparative analysis of specificity.

.	TP_40	TP_50	TP_60	TP_70	TP_80	TP_90
Random Forest	83.53175	82.77027	88.82979	94.68085	83.95062	85.57214
LGBM	87.01826	86.84211	91.28205	84.90566	88.26406	87.5
RFXG	88.16568	84.31373	91.58076	92.15686	90.75426	89.44724
CNN	89.85507	91.31833	89.3617	89.42308	87.03242	93.13725
LSTM	83.4	89.52703	83.41232	87.73585	85.82474	84.36019
Proposed CNN-LSTM	**91.15385**	**91.97324**	**95.05963**	**95.78947**	**96.0199**	**96.46465**

CONCLUSION

This study offers a comprehensive study on detecting DDoS attacks in IoT networks, with a particular focus on hybrid Deep Learning (DL) classifiers. With the rapid advancement of DL algorithms, innovative hybrid models have attracted considerable interest from researchers. By examining studies published between 2020 and 2024, the survey underscores the effectiveness of hybrid classifiers in combating DDoS attacks. Optimized hybrid classifiers demonstrate superior performance compared to general hybrid models across key metrics, highlighting the significance of customized strategies to address the particular difficulties posed by DDoS assaults in IoT systems. The proposed CNN-LSTM model's effectiveness is evaluated using various DDoS attack detection techniques, demonstrating superior performance. The model obtained 92.88% accuracy, 92.97% specificity, and 92.78% sensitivity. Increasing the training data further improved the model's performance, achieving 96.27% accuracy, 96.46% specificity, and 96.08% sensitivity. While DL algorithms hold significant promise for improving IoT security, challenges in detecting and mitigating DDoS attacks remain. As malicious tactics evolve alongside technology, ongoing research and innovation are crucial. Strengthening IoT networks against an ever-changing threat landscape remains a critical priority for the research community.

REFERENCES

1. Elsaeidy AA, Jamalipour A, Munasinghe KS. A hybrid deep learning approach for replay and DDoS attack detection in a smart city. IEEE Access. 2021 Nov 16; 9: 154864–75.
2. 3Javeed D, Gao T, Khan MT, Ahmad I. A hybrid deep learning-driven SDN-enabled mechanism for secure communication in Internet of Things (IoT). Sensors. 2021 Jul 18; 21(14): 4884.
3. 5Ullah S, Khan MA, Ahmad J, Jamal SS, e Huma Z, Hassan MT, Pitropakis N, Arshad, Buchanan WJ. HDL-IDS: a hybrid deep learning architecture for intrusion detection in the Internet of Vehicles. Sensors. 2022 Feb 10; 22(4): 1340.
4. 14Islam U, Muhammad A, Mansoor R, Hossain MS, Ahmad I, Eldin ET, Khan JA, Rehman AU, Shafiq M. Detection of distributed denial of service (DDoS) attacks in IOT based monitoring system of banking sector using machine learning models. Sustainability. 2022 Jul 8; 14(14): 8374.
5. 27Dabhade V, Alvi AS. Malicious Node Detection and Prevention for Secured Communication in WSN. In Computer Networks, Big Data and IoT: Proceedings of ICCBI 2021. Singapore: Springer Nature Singapore; 2022 May 22; 121–136.
6. 28Pabale AR, Kolhe RV, William P, Deshpande N, Paithankar DN, Yawalkar PM. Smart crack detection system using nanostructured materials with integrated optimization technology. J Nano-Electron Phys. 2023; 15(4): 04019. DOI: 10.21272/jnep.15(4).04019.
7. 29Panda M. Security in wireless sensor networks using cryptographic techniques. Am J Eng Res. 2014 Oct; 3(01): 50–6.
8. Sahu AK, Sharma S, Tanveer M, Raja R. Internet of Things attack detection using hybrid Deep Learning Model. Comput Commun. 2021 Aug 1; 176: 146–54.
9. Najafimehr M, Zarifzadeh S, Mostafavi S. A hybrid machine learning approach for detecting unprecedented DDoS attacks. J Supercomput. 2022 Apr; 78(6): 8106–36.

10. Alghazzawi D, Bamasag O, Ullah H, Asghar MZ. Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection. Appl Sci. 2021 Dec 8; 11(24): 11634.
11. Alzahrani MY, Bamhdi AM. Hybrid deep-learning model to detect botnet attacks over internet of things environments. Soft Comput. 2022 Aug; 26(16): 7721–35.
12. Sagu A, Gill NS, Gulia P, Priyadarshini I, Chatterjee JM. Hybrid Optimization Algorithm for Detection of Security Attacks in IoT-Enabled Cyber-Physical Systems. IEEE Trans Big Data. 2024 Mar 1; 11(1): 35–46.
13. Xinlong L, Zhibin C. [Retracted] DDoS Attack Detection by Hybrid Deep Learning Methodologies. Secur Commun Netw. 2022; 2022(1): 7866096.
14. Cil AE, Yildiz K, Buldu A. Detection of DDoS attacks with feed forward based deep neural network model. Expert Syst Appl. 2021 May 1; 169: 114520.
15. Alzahrani RJ, Alzahrani A. Security analysis of ddos attacks using machine learning algorithms in networks traffic. Electronics. 2021 Nov 25; 10(23): 2919.
16. Popoola SI, Adebisi B, Ande R, Hammoudeh M, Anoh K, Atayero AA. smote-drnn: A deep learning algorithm for botnet detection in the internet-of-things networks. Sensors. 2021 Apr 24; 21(9): 2985.
17. Niraja KS, Rao SS. WITHDRAWN: A hybrid algorithm design for near real time detection cyber attacks from compromised devices to enhance IoT security. Mater Today Proc. 2021 Mar 5. https://doi.org/10.1016/j.matpr.2021.01.751
18. Lakshmi Narayanan K, Santhana Krishnan R, Golden Julie E, Harold Robinson Y, Shanmuganathan V. Machine learning based detection and a novel EC-BRTT algorithm based prevention of DoS attacks in wireless sensor networks. Wirel Pers Commun. 2022 Nov; 127(1): 479–503.
19. Al-Taleb N, Saqib NA. Towards a hybrid machine learning model for intelligent cyber threat identification in smart city environments. Appl Sci. 2022 Feb 11; 12(4): 1863.
20. Wazzan M, Algazzawi D, Albeshri A, Hasan S, Rabie O, Asghar MZ. Cross deep learning method for effectively detecting the propagation of IoT botnet. Sensors. 2022 May 20; 22(10): 3895.
21. Ahuja N, Singal G, Mukhopadhyay D, Kumar N. Automated DDOS attack detection in software defined networking. J Netw Comput Appl. 2021 Aug 1; 187: 103108.
22. Mohmand MI, Hussain H, Khan AA, Ullah U, Zakarya M, Ahmed A, Raza M, Rahman IU, Haleem M. A machine learning-based classification and prediction technique for DDoS attacks. IEEE Access. 2022 Feb 17; 10: 21443–54.
23. Alkahtani H, Aldhyani TH. Botnet attack detection by using CNN-LSTM model for Internet of Things applications. Secur Commun Netw. 2021; 2021(1): 3806459.
24. Pokhrel S, Abbas R, Aryal B. IoT security: botnet detection in IoT using machine learning. arXiv preprint arXiv:2104.02231. 2021 Apr 6.
25. Abdulrahman NF, Singh MJ. Deep learning approaches for DDoS attack detection in communication networks and iot: A comprehensive review. J Kejuruteraan. 2025; 37(1): 323–33.
26. Thangasamy A, Sundan B, Govindaraj L. A Novel Framework for DDoS Attacks Detection Using Hybrid LSTM Techniques. Comput Syst Sci Eng. 2023 Jun 1; 45(3): 2553–2567.
27. Ullah Z, Arif F, Haq QM, Khan NA, Din IU, Almogren A, Khan MA, Alsaleh O, Guizani M. Hybrid CNN-LSTM Model for DDoS Attack Detection in Internet of Things-based Healthcare Industry 5.0. IEEE Internet Things J. 2025 May 13; 12(22): 46075–46082.
28. Mousa AK, Abdullah MN. An improved deep learning model for DDoS detection based on hybrid stacked autoencoder and checkpoint network. Future Internet. 2023 Aug 19; 15(8): 278.
29. Sadhwani S, Manibalan B, Muthalagu R, Pawar P. A lightweight model for DDoS attack detection using machine learning techniques. Appl Sci. 2023 Sep 2; 13(17): 9937.
30. Maguluri LP, Sorapalli YS, Nakkala LK, Tallari V. Smart street lights using IoT. In 2017 IEEE 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT). 2017 Dec 21; 126–131.
31. Rathod U. Role of Deep Learning in Mobile Ad-hoc Networks. Publications in Journal. 2022 Dec; 2022: 23.

