GMR
The Original

AN EFFECTIVE APPROACH FOR INTRUSION DETECTION IN IOT ENVIRONMENT

Ramesh Chandra Goswami[1*], Hiren Joshi[2]

[1*]Department of Computer Science ,Gujarat University ,Ahmedabad,Gujarat,India Email Id: rameshchandragoswami@gujaratuniversity.ac.in
[2]Department of Computer Science ,Gujarat University ,Ahmedabad,Gujarat,India Email Id: hdjoshi@gujaratuniversity.ac.in

Abstract:
The Internet of Things enables connectivity among heterogeneous physical devices and supports real-time applications in transportation, healthcare, military systems, and agriculture. However, extensive use of communication protocols exposes IoT networks to serious security threats, while traditional signature-based and rule-based intrusion detection techniques remain ineffective against evolving and unknown attacks. Accurate analysis of network traffic behavior is therefore essential for secure IoT operations. This paper presents an Intrusion Detection System (IDS) that is based on a deep learning framework that integrates feature selection based on correlation with a convolutional neural network (CNN) for anomaly detection in a network. Initially, the most informative traffic features are selected using a linear correlation-based extraction strategy to reduce redundancy and improve learning efficiency. The refined feature set is then processed by a convolutional neural network to automatically learn discriminative patterns associated with malicious activities. The proposed system supports both binary classification and multiclass classification for anomaly detection and for identifying different categories of attacks. The proposed approach is evaluated using multiple benchmark datasets representing diverse network environments. For comparison, several conventional machine learning classifiers, including linear discriminant analysis, k-nearest neighbors, classification and regression trees, and support vector machines, are trained using the same feature extraction strategy. Experimental evaluation confirms a significant improvement in the proposed model, which improves security performance in IoT environments.

Keywords: IoT Security, Network Intrusion Detection, Deep Neural Networks, Cyber Threat Analysis Network Security, Cyber Attack Detection, Anomaly Detection.

INTRODUCTION

Numerous smart gadgets used in homes, communities, healthcare, transportation, and industries are connected by the Internet of Things (IoT). These gadgets gather data in real time to support informed decision-making. However, the likelihood of cyberattacks rises with the number of linked devices. IoT systems are vulnerable to attacks like DDoS and botnets, thus safeguarding these gadgets is crucial [1].

IoT presents special issues that make traditional security measures ineffective. Intrusion Detection Systems are used to identify unusual activity or attacks in order to enhance security. IDS can identify attacks by searching for anomalous behavior (anomaly-based) or recognized patterns (signature-based). IDS becomes more intelligent and flexible because of machine learning and deep learning approaches. While machine learning models were successful in identifying threats in earlier studies, their accuracy and complexity were limited. In order to detect various assaults on IoT devices more accurately and with fewer false alarms, this study suggests a new deep learning model [2].

Large volumes of data are produced by IoT devices as they proliferate, enabling smarter and more effective services. Across numerous industries, automation, better decision-making, and improved user experiences are made possible by this data-driven connectedness. But the variety and size of IoT devices also present difficult security issues [3].

Strong security measures are challenging to deploy since many devices have limited memory and processing capacity. Furthermore, IoT networks frequently use decentralized topologies and a variety of communication protocols, which raises the possibility of vulnerabilities. Therefore, it is essential to provide strong security solutions designed especially for IoT contexts in order to guarantee user privacy and safety as well as the dependability of the linked systems. The number of gadgets connected by the Internet of Things is currently more than the number of people on the planet. IoT devices are utilized in a variety of industries, including farming, transportation, healthcare, and the military [4].

We evaluated our model on two widely used datasets and found that proposed model outperforms conventional machine learning techniques. In order to enhance IoT security, this study includes background, methodology, experimental results, and findings.

1.1 Intrusion detection system in IoT

The development of strong Intrusion Detection Systems (IDS) is crucial since traditional methods are unable to counteract the sophisticated cyberattacks that target IoT networks. IDSs employ methods including signature, specification, and anomaly-based detection to monitor network traffic across different IoT layers. Signature-based intrusion detection systems (IDSs) are effective against known threats but not against new ones. IDSs that are specification-based depend on pre-established rules, necessitating regular changes [5]. Although anomaly-based intrusion detection systems have a high false positive rate, they are capable of identifying fresh incursions. Because of their capacity to identify abnormalities and adjust to changing threats, machine learning (ML) and deep learning (DL) models have become increasingly popular as solutions to these problems [6]. To find abnormalities, current IDS techniques mostly use ML and DL models [7].

Scholars have employed datasets such as KDDCUP99[8], NSL-KDD [9], and UNSW-NB15[10], despite the fact that many of them are out-of-date or contain redundant features. Although ML models like Random Forest and SVM exhibit encouraging accuracy, they frequently have problems like overfitting and high false alarm rates. Although they frequently suffer from lengthy training cycles and increased complexity, DL approaches, such as RNNs, CNNs, and hybrid models like CNN-LSTM and GAN-based DNNs, have achieved high detection rates. To improve model performance, a number of researchers have also incorporated optimization approaches.

Meanwhile, many researchers continue to overlook practical IoT data issues. In order to address these problems, a novel IDS model that employs the CNN technique has been put forth. It emphasizes feature engineering, manages data imbalance, reduces overfitting, and increases detection accuracy in both binary and multiclass classification scenarios. Lastly, we contrast the model's performance and performance metric with those of conventional machine learning techniques. The comparison of Machine Learning Techniques on Common Intrusion Detection Datasets in shown in Table-1.

Table-1 Comparison of Machine Learning Techniques on Common Intrusion Detection Datasets

Dataset Used	Method Used	Output	Anomaly/Misuse/Attack Detected	Reference
CICIDS 2017	Decision tree ML model	96% detection accuracy	Binary	[11]
UNSW-NB 15	PCA with six ML classifiers	Evaluation using accuracy, F1-score, precision, etc.	Binary	[12]
UNSW-NB15, NSL-KDD	CNN + Bi-LSTM with SMOTE	Better performance with imbalanced data	Binary & Multiclass	[13]
UNSW-NB15	GAN-based DNN	84% accuracy on real data, 91% using synthetic data	Binary	[14]
KDD CUP 99	Weka	Accuracy of model between 87% to 100%	Multiclass	[15]
NSL-KDD	NB and SVM classifier	97% accuracy with SVM, 32–44% error with NB	Binary	[16]
NSL-KDD	RNN	80% accuracy	Binary & Multiclass	[17]
KDD CUP 99	CNN	Poor accuracy for U2R & R2L attacks	Multiclass	[18]
UNSW-NB15, CIDCC-001, NSL-KDD	FSO + LSTM	98% accuracy, high training time	Binary & Multiclass	[19]

2.0 METHODOLOGY

This study made use of two publicly accessible datasets. These datasets were chosen on the basis of their quality and applicability. Every dataset adds a different piece of information to the analysis. Below is a thorough description of each dataset.

3. DATASET DESCRIPTION

In this study two publicly available datasets are used. Each is given below.

3.1 IOTID20

IOTID20[20] is an academic dataset made from raw network packet files from IoT contexts that is accessible to the general public. It has an Internet of Things network configuration with smart home appliances like the EZVIZ Wi-Fi camera and NUGU AI speaker, as well as computers and smartphones linked via a Wi-Fi router. The dataset is intended to assist IoT security research and contains simulated assaults carried out with Nmap tool [21]. Four groupings comprise the attack types:

i).Mirai: Involves creating a botnet from compromised devices in order to carry out coordinated attacks.
ii).Denial of Service: Disrupts services to other devices by flooding the target server from a single source.
iii).Man-in-the-Middle ARP Spoofing: By placing themselves in the network path, attackers can intercept and alter data between two connected devices.

iv).Scan: During the scanning process, attackers try to obtain information about the devices and manipulate it.
The dataset contains a mixture of legitimate and malicious traffic distributed across several attack categories. Benign network activity accounts for 38,598 instances, representing normal operational behavior. Among the attack types, denial-of-service attacks are the most frequent with 59,390 instances, indicating intensive traffic flooding patterns. Mirai-based attacks also form a substantial portion of the dataset with 23,078 instances, reflecting malware-driven IoT exploitation. Scanning activities are represented by 56,744 instances, highlighting reconnaissance behavior, while man-in-the-middle attacks based on ARP spoofing appear less frequently with 25,868 instances, illustrating targeted interception attempts. For creating and assessing intrusion detection systems in smart home and Internet of Things network situations, this dataset is useful.

3.2 CICIDS2017

The CICIDS2017 [22] dataset is Canadian Institute for Cybersecurity at the University of New Brunswick created this popular benchmark dataset for examining network traffic in both benign and malevolent situations. It was gathered over the course of five days using ISCXFlowMeter, which transformed pcap files into CSV format. It has eighty features. Eleven different attack types—DoS,Botnet,Firewall, and Port Scan—are included in the dataset.

i).DoS attacks: This attack, which uses HTTP requests to overload systems, is simple to initiate and challenging to detect.
ii).Botnet attacks This attack uses malware-infected devices that are remotely controlled by attackers (botmasters) to carry out destructive tasks like DDoS without the victims' awareness.
iii).Port Scan attacks: This attack is executed using tools like Nmap, helps attackers gather system information such as OS, active services, and port statuses.
iv).Firewall category: FTP-Patator, SSH-Patator, and infiltration attacks that seek to enter systems remotely are all included in the firewall category.

The dataset consists of both malicious and benign network traffic instances distributed across multiple attack categories. Normal (benign) traffic forms the largest portion of the data, reflecting typical network behavior. Among the attack classes, denial-of-service attacks are the most prevalent, indicating a strong presence of high-volume disruptive traffic. Port scanning activities are also significant instances, highlighting reconnaissance-based attack behavior. In contrast, botnet and firewall-related attacks occur less frequently, demonstrating different classes of different attack types within the dataset. The dataset is valuable for training and evaluating intrusion detection systems in cybersecurity research.

4.THE WORKFLOW

4.1 Data pre-processing

Data pre-processing, sometimes referred to as data cleaning or massaging, entails resolving missing information, eliminating redundant characteristics, and combining sub-attacks into primary attack categories. Binary (two classes) and multiclass (five classes, including normal) classifications are applied to the data. Lastly, normalization (0–1 range) is used to lower computing complexity and guarantee compatibility across various techniques.

4.2 Feature Selection

By eliminating unnecessary data and cutting down on overfitting and training time, feature extraction is essential for enhancing the precision and effectiveness of ML/DL models. The suggested model ranks and chooses features according

to their association with the target class using a feature importance method based on the Pearson Component Coefficient. A dataset-specific correlation threshold is utilized to exclude less important features in a three-stage procedure that includes correlation calculation, attribute ranking, and feature selection.

5.PROPOSED MODEL

The proposed model is a lightweight and effective intrusion detection system that uses a convolutional neural network for classification and the Pearson Correlation Coefficient for feature selection. A filter-based technique effectively chooses pertinent features, which are subsequently fed into the CNN. Using ReLU and Softmax activation functions, the Convolutional Neural Network architecture consists of three convolutional layers, pooling layers, flattening layers, and dense layers. The model was trained for binary classification and for multiclass classification, In both classifications, the model was optimized using the Adam optimizer.

6.EVALUATION CRITERIA

Model evaluation is essential for choosing the best method. It guarantees that the selected method is appropriate for the datasets and applications. Important metrics consist of

i)Confusion Matrix:

A table used to assess a classification model's performance (particularly in supervised learning) is called a confusion matrix. To determine how frequently the model is accurate or inaccurate, it compares the actual labels with predicted labels of the model.

A confusion matrix divides the predictions made by a classifier into four main parts. True Positives (TP) are instances in which the model accurately predicts the positive class, indicating that the item actually falls into the positive category and is recognized as such by the model. In contrast, True Negatives (TN) occur when the model accurately predicts the negative class for objects that are actually negative.

False Positives(FP) happen when the model predicts something as positive when it is actually negative. False Negatives (FN) occur when the model fails to identify a true positive and instead classifies it as negative. Together, TP, TN, FP, and FN give a complete picture of a model's performance by displaying both how and where it makes errors in addition to how often it is correct.

ii)**Accuracy:** A performance indicator called accuracy indicates how frequently a model delivers accurate predictions. It is the percentage of all predictions—true positives and true negatives—that come true out of all the examples. Simply said, accuracy gauges the model's overall performance. Mathematically it is expressed as:

$$\text{Accuracy}=(TP+TN)/(TP+TN+FP+FN) \quad -----1$$

It indicates the percentage of accurate predictions made by the model.

ii)Precision and Recall: Precision is the number of favorable outcomes that the model accurately predicted. It emphasizes the caliber of optimistic forecasts. Precision can be expressed as follows:

$$\text{Precision}=TP/(TP+FP) \quad ----------2$$

The model produces very few false-positive errors when its precision is high.

The proportion of real positive cases identified by the model is known as recall. It emphasizes how the model can identify every positive.

$$\text{Recall}=TP/(TP+FN) \quad ----------3$$

A high recall indicates that relatively few true positives are missed by the model.

iii)F1-Score:

A statistic called the F-1 score uses the precision and recall harmonic means for creating a single figure. It is particularly helpful when the dataset is unbalanced, or you need to strike a compromise between recall and precision. It can be mathematically expressed as:

$$\text{F1-Score}=(2*\text{Precision}*\text{Recall})/(\text{Precision}+\text{Recall}) \quad ----------4$$

The F1-score only increases when both precision and recall are good since it makes use of the harmonic mean. The F1-score will be low if one of them is low. Because of this, it's a useful metric for assessing how successfully a model detects positives while preventing an excessive number of false alarms.

6.1 Binary Classification:

This classification is a learning approach in which observations are separated into one of two possible outcomes. It is commonly applied when the objective is to decide whether activity is legitimate or indicative of an intrusion.

Table 2: Binary classification accuracy

ML models	IOTID20	CICIDS2017
LDA	0.91	0.93
KNN	0.97	0.97
CART	0.97	0.96
SVM	0.92	0.87
Proposed Model	0.99	0.98

Table 3: Performance metrics for Binary Classification

Dataset	IoTID20			CICIDS2017		
ML Models	Precision	Recall	F1-Score	Precision	Recall	F1-Score
LDA	0.57	0.50	0.89	0.92	0.96	0.91
KNN	0.95	0.96	0.94	0.95	0.94	0.94
CART	0.95	0.94	0.97	0.96	0.94	0.94
SVM	0.65	0.94	0.94	0.87	0.93	0.85
Proposed Model	0.97	0.97	0.96	0.97	0.98	0.99

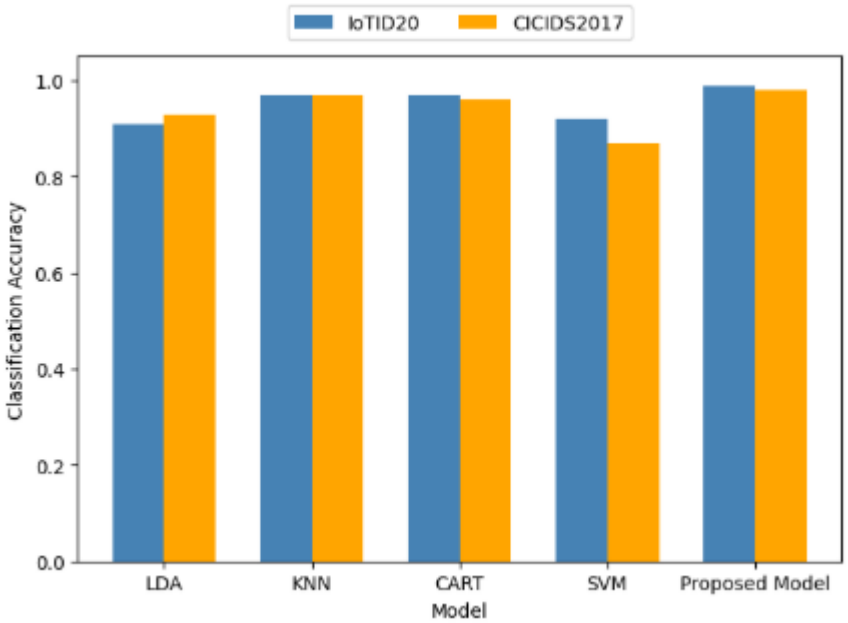

Figure-1 Binary Classification for Accuracy Comparison

6.2 Multiclass Classification:
Multiclass classification assigns observations to one category from several predefined classes. This technique is used when distinguishing among multiple attack behaviors rather than making a simple normal-versus-attack decision.

Table 4: Classification accuracy of Multiclass classification

ML models	IOTID20	CICIDS2017
LDA	0.73	0.91
KNN	0.96	0.97
CART	0.97	0.97
SVM	0.83	0.65
Proposed Model	0.92	0.96

Table 5: Multiclass Classification performance metrics

ML Models	IOTID20			CICIDS2017		
ML models	Precision	Recall	F1-Score	Precision	Recall	F1-Score
LDA	0.74	0.72	0.73	0.9	0.91	0.91
KNN	0.96	0.96	0.96	0.97	0.96	0.96
CART	0.96	0.97	0.98	0.96	0.96	0.96
SVM	0.86	0.84	0.84	0.76	0.67	0.68
Proposed Model	0.86	0.86	0.85	0.87	0.68	0.72

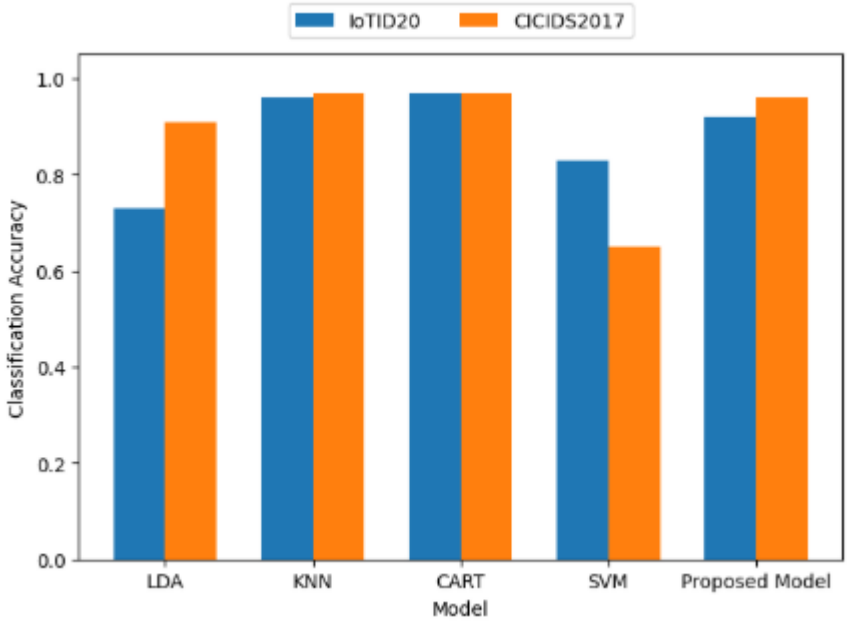

Figure-2: Multiclass classification Accuracy Comparison

7. RESULTS & DISCUSSION
Results of evaluating different machine learning models for binary and multiclass intrusion detection tasks. The IOTID20 and CICIDS2017 datasets are used to evaluate the performance in order to determine its efficacy and efficiency in practical situations. Eighty percent of the data was utilized for training, while twenty percent was used for testing. The proposed

deep learning model and the supervised machine learning classifiers such as LDA, KNN, CART, and SVM were trained and evaluated for performance comparison on each dataset, with the proposed model .

7.1 Binary classification

The experimental results show that the proposed model outperforms the existing machine learning approaches on both the IOTID20 and CICIDS2017 datasets. It achieves the highest accuracy while maintaining reasonable computational time, making it suitable for practical intrusion detection applications. Although models such as KNN and CART achieve comparable accuracy, their higher execution time limits their efficiency. Overall, the balanced performance of the proposed model in terms of accuracy, precision, recall, and F1-score demonstrates its effectiveness for binary classification in network security systems.

7.2 Multi-class classification

The multiclass classification results show that CART and KNN provide the highest accuracy across both datasets, though KNN requires higher computational time. The proposed model demonstrates stable and balanced performance with moderate execution cost. In contrast, SVM shows lower accuracy and high processing time, limiting its practicality. Overall, models that balance classification performance and computational efficiency are more suitable for multiclass intrusion detection tasks.

8.CONCLUSION

The efficiency of the assessed models on the IOTID20 and CICIDS2017 datasets is demonstrated by the experimental results from both multiclass and binary classification tasks. The suggested model regularly achieves high accuracy in binary classification, this qualifies it for use in practical intrusion detection applications. KNN and CART are likewise quite accurate. While the proposed model offers consistent and balanced performance with minimal processing requirements, CART and KNN exhibit good predictive potential for multiclass classification. SVM, on the other hand, shows far higher computational cost and poorer classification results in both situations. Overall, the study emphasizes how crucial it is to choose models for real-world network security systems that preserve a reasonable computing complexity while achieving dependable detection accuracy.

9.DECLARATION OF AI USAGE

This article uses some tool like QuillBot for improving language and sentence structure. All conceptualization, analysis, interpretation, and scientific content were entirely performed by the authors.

10.AVAILABILITY OF DATA AND MATERIAL

Dataset are collected from open source.

10.1. Declarations

10.2 Ethical approval and participation consent

Ethical approval and consent to participate were not required for this study.

10.3 Consent for publication

Consent for publication is not applicable.

10.4 Clinical trial registration

This study was not registered as a clinical trial.

10.5 Competing interests

The authors confirm that there are no competing interests.

10.6 Funding

No funding was received for this research.

11. CONFLICT OF INTEREST STATEMENT

The authors state that no conflicts of interest exist in relation to this work.

REFERENCES

1. C. Zhong, Z. Zhu, and R.-G. Huang, “Study on the IOT Architecture and Access Technology,” in 2017 16th International Symposium on Distributed Computing and Applications to Business, Engineering and Science (DCABES), 2017, pp. 113–116. doi: 10.1109/DCABES.2017.32.

2. B. Raviprasad, C. R. Mohan, G. N. R. Devi, R. Pugalenthi, L. C. Manikandan, and S. Ponnusamy, “Accuracy determination using deep learning technique in cloud-based IoT sensor environment,” Measurement: Sensors, vol. 24, p. 100459, 2022.
3. R. Krishnan, P. Rajpurkar, and E. J. Topol, “Self-supervised learning in medicine and healthcare,” Nat. Biomed. Eng., pp. 1–7, 2022.
4. D. Shah, A. Singh, and S. S. Prasad, “Sentimental Analysis Using Supervised Learning Algorithms,” in 2022 3rd International Conference on Computation, Automation and Knowledge Management (ICCAKM), 2022, pp. 1–6.
5. S. Anwar et al., “From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions,” Algorithms, vol. 10, no. 2, p. 39, 2017.
6. A. Shaver, Z. Liu, N. Thapa, K. Roy, B. Gokaraju, and X. Yuan, “Anomaly based intrusion detection for IoT with machine learning,” in 2020 IEEE applied imagery pattern recognition workshop (AIPR), 2020, pp. 1–6.
7. H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, “Intrusion detection system: A comprehensive review,” Journal of network and computer applications, vol. 36, no. 1, pp. 16–24, 2013.
8. F. A. Bakhtiar, E. S. Pramukantoro, and H. Nihri, “A Lightweight IDS Based on J48 Algorithm for Detecting DoS Attacks on IoT Middleware,” in Proceedings of the 2019 IEEE 1st Global Conference on Life Sciences and Technologies (LifeTech), IEEE, Mar. 2019, pp. 41–42. doi: 10.1109/LifeTech.2019.00017.
9. A. Anish Halimaa and K. Sundarakantham, “Machine Learning Based Intrusion Detection System,” in Proceedings of the 3rd International Conference on Innovations in Engineering and Technology (ICOEI), IEEE, 2019.
10. N. Moustafa and J. Slay, “UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems,” in 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, ACT: IEEE, 2015, pp. 1–6.
11. M. A. Ferrag, L. Maglaras, A. Ahmim, M. Derdour, and H. Janicke, “Rdtids: Rules and decision tree-based intrusion detection system for internet-of-things networks,” Future Internet, vol. 12, no. 3, p. 44, 2020.
12. Y. K. Saheed, A. I. Abiodun, S. Misra, M. K. Holone, and R. Colomo-Palacios, “A machine learning-based intrusion detection for detecting internet of things network attacks,” Alexandria Engineering Journal, vol. 61, no. 12, pp. 9395–9409, 2022.
13. K. Jiang, W. Wang, A. Wang, and H. Wu, “Network intrusion detection combined hybrid sampling with deep hierarchical network,” IEEE access, vol. 8, pp. 32464–32476, 2020.
14. B. Sharma, L. Sharma, C. Lal, and S. Roy, “Anomaly based network intrusion detection for IoT attacks using deep learning technique,” Computers and Electrical Engineering, vol. 107, p. 108626, 2023.
15. I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, “Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy,” in 2019 international carnahan conference on security technology (ICCST), 2019, pp. 1–8.
16. A. Halimaa and K. Sundarakantham, “Machine learning based intrusion detection system,” in 2019 3rd International conference on trends in electronics and informatics (ICOEI), 2019, pp. 916–920.
17. C. Yin, Y. Zhu, J. Fei, and X. He, “A deep learning approach for intrusion detection using recurrent neural networks,” Ieee Access, vol. 5, pp. 21954–21961, 2017.
18. Y. Xiao, C. Xing, T. Zhang, and Z. Zhao, “An intrusion detection model based on feature reduction and convolutional neural networks,” IEEE Access, vol. 7, pp. 42210–42219, 2019.
19. A. S. Alqahtani, “RETRACTED ARTICLE: FSO-LSTM IDS: hybrid optimized and ensembled deep-learning network-based intrusion detection system for smart networks,” J. Supercomput., vol. 78, no. 7, pp. 9438–9455, 2022.
20. H. Kang, D. H. Ahn, G. M. Lee, J. Do Yoo, K. H. Park, and H. K. Kim, “IoT network intrusion dataset,” 2019, IEEE Dataport. doi: 10.21227/q70p-q449.
21. A. Bhardwaj, “Network Intrusion Detection Using Machine Learning,” 2022.
22. I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization,” in Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP), Portugal, Jan. 2018.