JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 09 Issue 02
2025

Research Article
https://doi.org/10.56979/902/2025

Enhancing Intrusion Detection in AIOT using Intelligent Feature Selection and Deep Learning Fusion

Umair Abid[1*], Naeem Aslam[1], Ahmed Naeem[1], Muhammad Fuzail[1], and Muhammad Imran[1]

[1]Department of Computer Science, NFC-IET, Multan, Pakistan.
[*]Corresponding Author: Umair Abid. Umairabid12344@gmail.com

Received: June 10, 2025 **Accepted:** July 30, 2025

Abstract: As the industrial IoT and AIoT continue to rapidly advance, new security concerns have arisen as a result of the exponential growth in the volume of data transmitted via communication networks. When it comes to evolving cyberthreats, traditional safeguards like encryption and firewalls are often not enough. As a result, intrusion detection systems (IDS) are now essential for ensuring secure and reliable Internet of Things connectivity. This paper proposes a system that combines deep learning (DL) models with PCA and several feature selection procedures to enhance real-time intrusion detection. In order to improve classification performance and reduce dimensionality, five feature selection methods were evaluated and combined with principal component analysis (PCA): symmetrical uncertainty (SU) & Pearson analysis. Multiple classifiers were applied to the RT-IoT2022 dataset, including TabNet, DNNs, and ANNs. When compared to ANN (92.3614% accuracy) and TabNet (94% accuracy), the combined performance of ANN, Pearson analysis, and PCA (98.6123% accuracy) was much better. Key attributes discovered were responsible for the performance increases. The results demonstrate that a powerful method for identifying threats in real-time AIoT environments may be achieved by integrating PCA with efficient feature selection, which in turn increases the accuracy and efficiency of IDS.

Keywords: Cybersecurity; Internet of Things; Intrusion Detection System (IDS); Anomaly Detection; Security Attacks; Deep Learning

1. Introduction

Deep learning (DL) techniques employ many operators, proving advantageous for diverse mechanisms, particularly the ANN. It consists on 3 layers[2], [3]. In deep learning operates nonlinearly, generating responses received from the input layers. Recently, deep learning methodologies have been increasingly employed for speech recognition. Deep learning methodologies are extensively employed in the fields of genomics and medicine for illness analysis. The architecture and operation of deep learning methods utilize intricate data organization (including images, text, and numerical hierarchies) and demonstrate the management of large datasets through forward and backward propagation techniques. Furthermore, the subsequent inquiry addresses how devices alter the values and hyperparameters associated with dimensions to calculate the size of samples, so affecting the various layers. Effective techniques create a subtle distinction between the presentation and representation of testing and training. characteristics of obsolete wisdom stem from a slight divergence family's customary qualitative and fundamentals methodologies [5].

An IDS is employed safeguard interface interaction and detect intrusions within network. Numerous Intrusion Detection Systems (IDSs) have been developed for safe internet communication [6]. Upon detection of malicious activity on the network, it actively monitors and alerts the system administrator. IoT devices are small and mobile, rendering them suitable for remote areas [7]. Nonetheless, the computational capability is constrained by its diminutive dimensions and insufficient battery capacity. Moreover, they

convey information via lightweight protocols [8]. Developing a resilient model that effectively identifies intrusions in direct time when network stats fluctuates dynamic circumstances is more difficult [9]. Numerous academics have attempted to develop an ids undergoing training a particular data- type. Certain outcomes remarkable on certain dataset; yet, implementing produced IDS may prove difficult in direct time due to potential discrepancies between actual traffic and the dataset [10]. Most Intrusion Detection Systems (IDS) are trained on extensive datasets, yielding precise outcomes on which the model is deployed. Nonetheless, the data utilized for training complicates the ability to collect same properties [11].

The deep learning methods must not disclose critical or confidential information. An intrusion detection system is typically a software application or a hardware device that monitors incoming and outgoing network traffic for indications of malicious activity or breaches of security protocols [12]. Intrusion detection systems and IDS solutions are sometimes likened to intruder alarms, notifying managers of any activities that could jeopardize data or network infrastructures [13].

Intrusion Detection System (IDS) programs analyze network packets and visitor patterns to identify anomalous behavior or signs of potential compromise. Intrusion detection systems are predominantly passive, while some can take action upon detecting malicious behavior [14]. Primarily, they are designed to obtain real-time visibility during instances of capacity community compromises. Various IDS items exhibit distinct responses based on the sort of intrusion detection apparatus that has been implemented [15]. A NIDS, will strategically deploy sensors throughout network. it thereafter identify socialization visits without inducing performance difficulties or obstructions. HIDS function designated devices & servers, effectively monitoring access to those particular devices and hosts [16].

Customary intrusion detection systems rely on two main methods: anomaly based detection and signature based detection. Significance of signature-based intrusion detection systems (IDS) in detecting known threats is dependent on their ability to compare observed network or system behavior with a database of previously identified attacks [17]. When it comes to detecting new or unknown threats, this method has its own set of issues, but it works well for identifying attacks that fit earlier patterns. Keeping the signature database up-to-date with the latest threat signatures is a challenge in diverse and constantly evolving IoT contexts [18]. 1) establishing a baseline of typical behavior and 2) using any departures from the baseline to alert of potential breach is how anomaly-based intrusion detection systems function. Due to the broad variety of daily actions, this technique may produce a high number of false positives; nonetheless, it is helpful in detecting new, undetected dangers with unknown signatures. When device behaviors are diverse in IoT environments, handling false positives becomes more challenging [19,20].

2. Literature Review

In the study [21] indicated a new hybrid feature-selection approach benefits of filter techniques for better classification accuracy. First, a filter approach reduces the dimensionality of feature vectors by aggressively selecting relevant features with statistical methods. This selection is then further refined using a wrapper approach that evaluates the performance of the machine learning models on the selected features , improves accur without losing economy, and we experiment this method on several applications including cyberattack detection on IoT data and emotion analysis. Authors [22], to enhance IDS in wireless IoT, studied statistics & Correlation-based selected features. It hints at a hybrid intrusion detection system that makes use of Random Forest classifier for misuse detection and anomaly detection using k-means clustering. The approach works effectively for standard attack classes in the Aegean Wi-Fi dataset, such as flooding and impersonation, and it seeks to decrease the false positive rates while enhancing the detection results.

Another study[23] presents intrusions in RPL-based configurations implicated hostile through Heterogeneous surveillance infrastructure published in [24]; their methodology assigns detection responsibilities to high-order nodes exclusively tasked with passive network monitoring. The scalability of the proposed approach is assessed through a deployment mechanism for monitoring nodes. Kesswani and Agarwal et al. introduce SmartGuard, an IDS-based system capable of identifying malicious threats both internally and outside within the network.

Authors. [25] developed a collaborative blockchain-based signature intrusion detection system, a comprehensive framework for safeguarding signature sharing in IoT environments against malicious

nodes. The fundamental idea is to progressively develop a delegated signature database utilizing blockchain technology. A collective IoT network can enhance detection efficacy by utilizing solely trusted and verified signatures. The primary objective of this study [26] is to employ a disagreement-based technique for intrusion detection. They also developed DAS-CIDS to improve detection and filter alerts, considering the characteristics of IoT networks.

This article [34] presents a way for detecting anomalies in IoT networks to mitigate data imbalance, The study examined existing systems principal assessment factor, encompassing workloads, metrics, and methodologies provide cybersecurity intrusion detection. Our study focuses on deep learning methods for intrusion detection in cyber security, as well as four additional papers [23, 28-31]. Conversely, many studies fail to offer a comparative analysis of DL Algorithms. Proposed paper represents inaugural comprehensive analysis of deep learning for Intrusion Detection Systems (IDS), encompassing methodology, datasets, and comparative evaluations, to the best of our knowledge.

3. Proposed Methodology

3.1. Dataset Description

For this study, the RT-IoT2022 dataset was utilized. Located in the UCI Machine Learning Repository, it is freely available to you [38]. A large number of real-time Internet of Things (IoT) devices, including Amazon Alexa and MQTT, contributed to the display of network traffic statistics we obtained set of features and tested them with the same classifiers. After that, we used principal component analysis (PCA) on the reduced dataset that was created by the feature selection methods. Using deep learning classifiers, we were able to validate the PCA matrix. We used the F1 score, recall, precision, and accuracy to evaluate the experimental results once we obtained them. In Figure 1, we can see the suggested model. The research was carried out using a Windows-based operating system with 32 GB RAM and an Intel® CoreTM i5 CPU @ 3.2 GHz. We used sklearn, Keras, and pytorch tabnet in addition to the standard Python packages. The optimal tabnet classifier parameters are displayed in Table 2.

Table 1. Optimized setup TabNet

Parameter	Reconfigured value consideration
No of Decis-Step	7
Relaxation Fact	1.2
Sparsity(Cof)	0.0005
Optimizer	AdamW
Initital Learn Rate	0.01
Training Size	512
Total no of Training Epochs	150

3.2. Feature Selection:

The extraction of relevant data from extensive datasets particular attention to machine learning data exploration fellowships [40]. Analysts acknowledge that Feature-Selection is a crucial element of efficient data analytics [41], as employing characteristics not invariably beneficial for classification activities. Data preparation involves the collection and manipulation of electronic data, as well as the transformation of info paramteters within specific set of data alteration of information perceived spectator, intended enhance acquisition data. There exists significant disparity concerning least and maximum numbers in data frames. Standarization procedure diminishes algorithmic and data complexity, hence facilitating improved outcomes for classification algorithms associated with neural networks. [42].

PCA is one of the most scientific disciplines rely on as a feature extraction method [44]. In order to derive a new set of characteristics called principal components, this nonparametric technique employs a linear transformation to glean crucial information from intricate datasets. By choosing components that optimize the dataset's variance, principal component analysis (PCA) aims to discover the most significant data variables. This minimizes feature reduction with little information loss.

3.3. Deep Learning Methods of Data Classification:

Classification represents a compelling domain within deep learning. Recently, numerous proposed categorization algorithms, including ANN, TabNet, and DNN, have been evaluated across various domains. They are succinctly outlined in the subsequent sections.

3.3.1. ANN:

The ANN model is a standard neural network model that uses math and mimic the way the brain's neural networks work [45]. Artificial neural networks have neuronal units that are connected to each other and are arranged in layers, just like the brain. Figure 2 shows how the computations were shown in this study as a transfer function in the output layer.

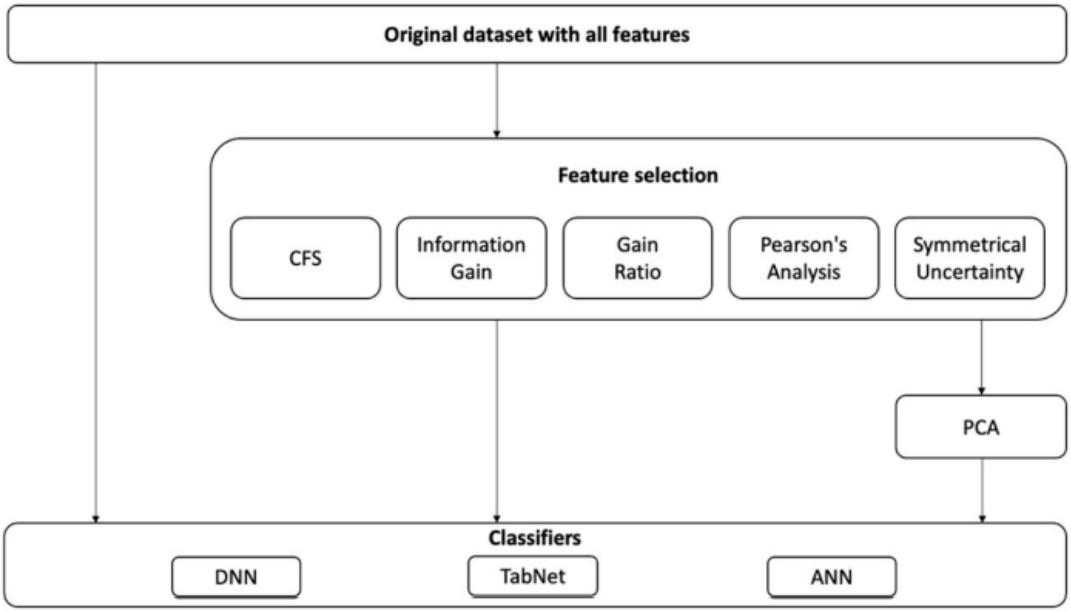

Figure 1. Diagram of the Proposed Predictive Network Detection Model

3.3.2. DNN

There are hidden layers in a DNN that exist between the input and output layers. This well-known deep learning method has been used in many scientific domains because it does a better job of selecting features and learning how to map difficult data. More hidden layers usually make the model work better. Every layer uses its own methods for sorting and classifying.

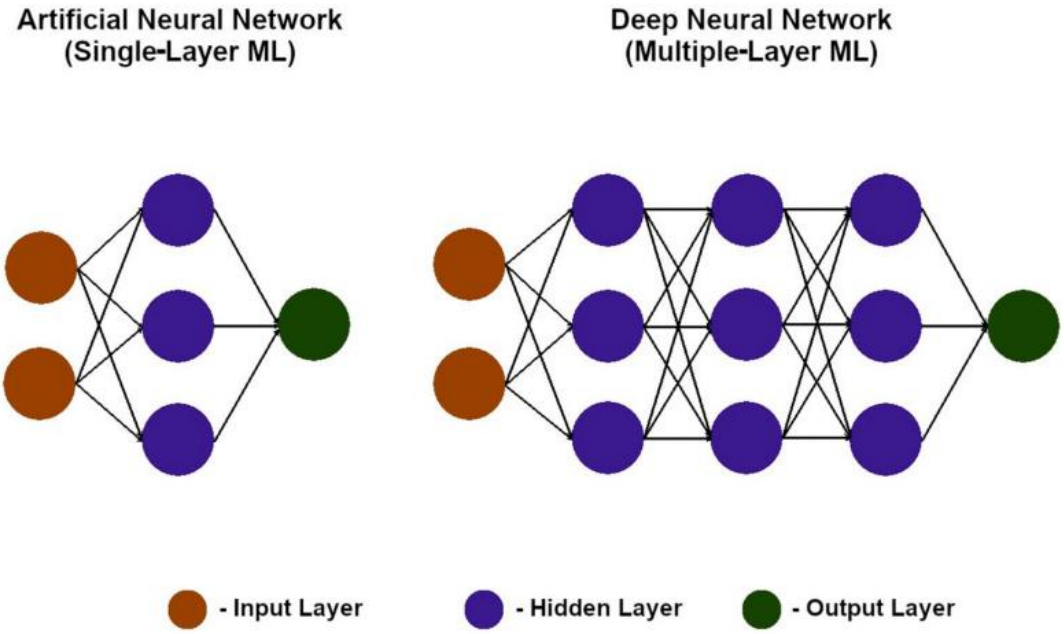

Figure 2. Representations of the ANN and DNN Architectures

3.3.3. Tabnet:

TabNet [46] is a new deep learning system that works from start to finish and was made just for tabular data. It shows how decision trees choose features by usage of Sequential based Attention methodology to choose features at each decision point. By giving learning power to the most important attributes, this method makes the model more useful and easier to understand. Figure 3 shows that the

TabNet encoder architecture has three main tasks at each step: feature transformation, attentive transformation, and masking. Because of this, TabNet gets rid of the need to deal with missing values during the data preparation phase [47].

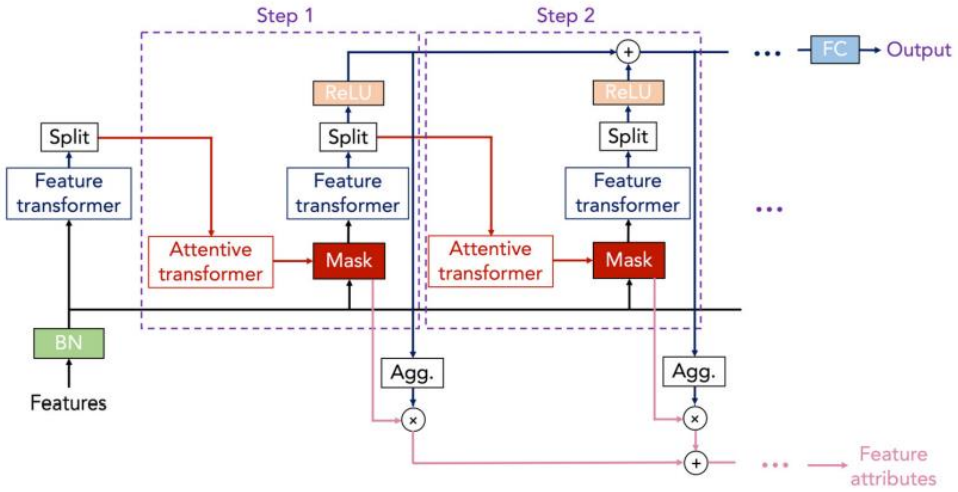

Figure 3. TabNet Encoder Architecture

4. Results & Discussion

This study utilized the RTIoT22 dataset to gather activities of network statistics from diverse IoT peripherials, comprising 113,125 instances. It sought to accurately analyze data to identify anomalous trends and so avert criminal activities. Firstly dataset divided into two regions: 70% designated as training ensemble and 30% as test samples for trials swift expansion of applications and network utilization has rendered security a paramount disputes surrounding network systems.A multitude of IoT devices depend on a self-generated system, vulnerable to various attacks. The network layer is susceptible to DoS attacks, entryway intrusions, packet sniffing, unauthorized access. Intrusion Detection Systems (IDS) are enhanced with advent of extensive, high-dimensional Internet of Things (IoT) and computer based networks.

This part, assessed outcomes of suggested setup. To discuss efficacy of a deep learning-contingent methodology for securing edge IoT devices within enterprise network environments.

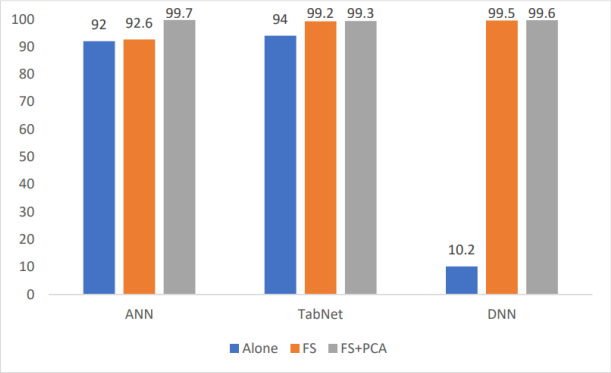

Figure 4. Classification Accuracy Comparison

4.1. Experiments Utilizing Solely Deep Learning Classifiers:

Before using feature selection methods, Table 2 shows how well the three deep learning classifiers worked.

Table 2. Outcomes of employing deep learning classification methods

Classifier	Accuracy(%)	Precision(%)	Recall(%)	FScore(%)
ANN	92.66	93.55	92.15	92.99
Tabnet	91.33	90.15	94	93.21
DNN	10.00	10.11	10	20

4.2. Experiments Utilizing Feature Selection Techniques with Deep Learning Classifiers:

The identical algorithms implemented alongside featureselection techniques. Initially, we implemented four featureselection algorithms The feature 'fwdinitwindowsize' utmost significant in predicting network behavior, was present in all feature selection methodologies. Next, feature selection strategies were used in conjunction with the same classification algorithms. We began by using five different methods for feature selection. All feature selection approaches included the 'fwdinitwindowsize' feature, which made the most significant prediction about the network's behavior. Feature selection methods were used to develop the classification algorithms. It demonstrates how well aspects picked classification methods using distinct feature selection tactics perform. A 92.6% accuracy rate was achieved by the ANN that used the SU approach. When feature selection for the ANN did not yield a noticeably better result. Despite TabNet's significantly worse accuracy (63% vs. 100%) while using CFS, which indicates a large number of misclassifications, TabNet's performance was much improved when using alternative feature selection methods. Compared to TabNet without feature selection created may have limited TabNet's detect optimal feature interactions, resulting in lower efficiency. When using feature selection approaches, DNN frequently demonstrated improved performance. Notably, a 99.5% accuracy rate was achieved by the DNN using GR. Applying stratified predictor variables allowed these models to demonstrate significant effectiveness. These models exhibited considerable efficacy through the application of stratified predictor variables.

4.3. PCA and feature selection with DL classifiers Experiments

First, we examined PCA idle and PCA through among the five feature selection approaches. Fig 5 displays the components from numerous feature selection strategies. Figure indicates that PCA plus feature selection yields better results than PCA alone.

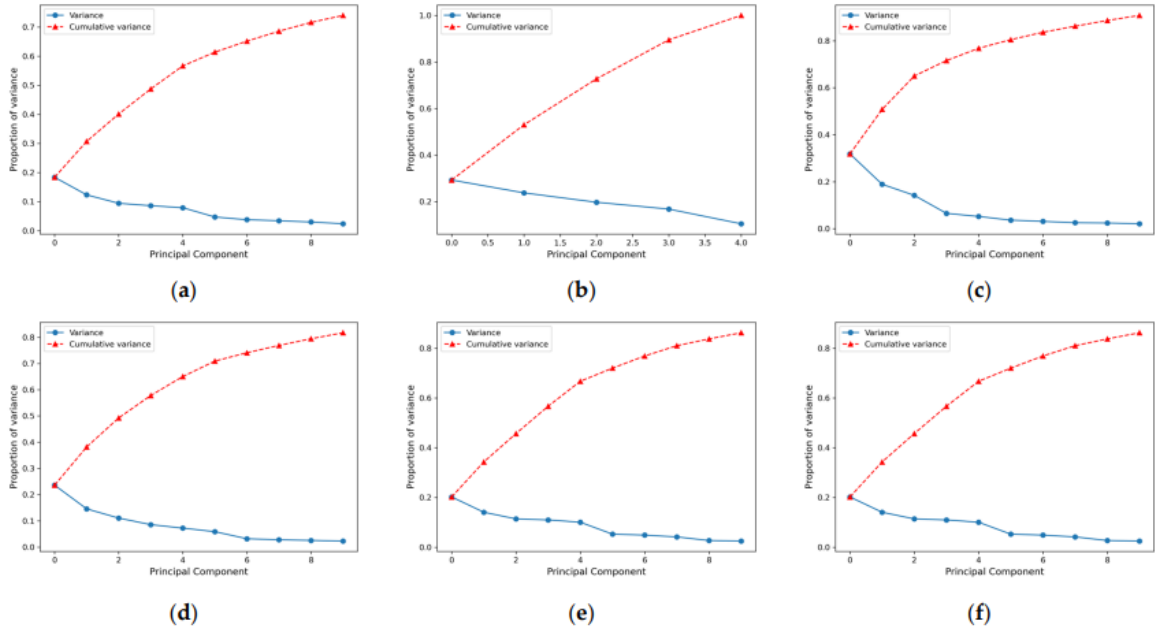

Figure 5. Analysis of the cumulative variances

Continuous network connectivity and data interchange are prerequisites for the widespread deployment of IoT devices in many different domains, such as smart cities, healthcare, and a plethora of industries. As a result, hackers may simply target Internet of Things devices and use them to compromise other devices on the same network. Both public and private sectors must work together to anticipate intrusions in order to mitigate the social and economic effects of numerous kind of network assaults [48].

Early identification of anomalous activity inside a network might provide prompt measures that may prevent activities. Not beyond mitigates risk of attacks but also enhances consumers' assurance in utilizing IoT devices, hence decreasing total security expenditures.

The present study demonstrates the capability of machine learning and deep learning to improve intrusion detection through a novel methodology that integrates the advantages of many predictive techniques [49]. In numerous practical situations, acquiring comprehensive network activity statistics might be difficult. Consequently, the initial step in developing an efficient IDS is the selection of a suitable and current dataset. It encompass specifically normative & anomalous actions replicate real-world

scenarios. Proposed method utilized the dataset RTIoT-22, Dataset encompasses many threats. The properties employed to distinguish between common and nefarious transmissions [39]. The selection of methodologies crucial in investigation guarantee robust IDS efficacy. The chosen methodologies Artificial Neural Networks, Deep Neural Networks, & TabNet. Their findings align other studies, indicating potential of these strategies to assist in intrusion detection [50–52].

Shorten processing times and reduce memory consumption by a large margin by reducing the attributes from 83 to a range of 5-32. When it comes to real-time systems, where efficiency is key, this reduction is a huge boon [53]. Using feature selection techniques in conjunction with PCA improved intrusion prediction in almost every case. When PCA was used in conjunction with Pearson analysis, the results were quite encouraging. All classifiers performed admirably when Pearson-PCA was used, however this does not mean that their efficacy is best when dealing with a large number of features. With a precision of 99.7 percent, the Pearson-PCA combined with ANN model was the most effective prediction tool. Our suggested model nearly satisfies the performance requirements for real-world AIoT deployments, which is why the accuracy of 99.7 percent is so crucial. Since assault patterns and network settings are always evolving scenarios remains exhausting. In light of this, it is clear that new and varied datasets are essential for the ongoing improvement and validation of models. The proposed model significantly improved prediction rate and accuracy while drastically reducing false positive rate by utilizing a variety of evaluation indicators. Instead of depending only on signature-dependant methods for improved IDS, this study emphasizes the necessity of using anomaly detection techniques.

Proposed study accomplished considerable accuracy on RTIoT-2022 dataset; however, real-world application requires continuous retraining with new data to adapt to changing threat patterns.

Future study should assess the model's efficacy using novel and diverse datasets or in real-time network settings. Ultimately, to evaluate the efficacy of our suggested model, we post it with the machine learning and deep learning methodologies outlined in the latest intrusion detection research. The suggested model accurately detected anomalous activity and surpassed alternative methods in the hold-out tests, as demonstrated in Table 3.

Table 3. Comparison of proposed methods to current intrusion detection systems.

Ref	Dataset	Adopted Models	Accu
[26]	NSL-KDD dataset	ILSTM	93.0900
[23]	ISCX-IDS, UNSWNB15	OCNN-HMLSTM	90.6755
[19]	RT-IoT2022	Combined feature selections-MLP	96.4441
Proposed Study	RT-IoT2022	Pearson-PCA with ANN	98.6123

Despite our methodology's superior performance, this investigation did not employ oversampling procedures to address dataset disparities. Therefore, in order to further authenticate and increase the model's robustness, further research will center around implementing oversampling techniques, such SMOTE.

5. Conclusion & Future Work

The goal of this study was to find the best way to lower no of dimensions to predict unusual patterns of network activity. It is not practicable to use a whole set of criteria to evaluate system assets. We suggested using PCA with feature selection methods to make DL algorithms better at predicting strange patterns of network activity. We chose five of the 83 input criteria and got good results in predicting invasions. The Pearson–PCA combined with ANN was the best of the predictive models, with an accuracy of 98.6123%. The Pearson analysis showed that some features related to the type of attack in network traffic. Our method can be used in a number of real-world situations where anomaly-based IDSs need to look at large datasets and find risk indicators that go along with them. Because the classes in the dataset used in this work are not evenly distributed, the trained model may be biased. In the future, researchers should apply oversampling methods to reduce overfitting, shorten the training time, and make the suggested model more accurate. This means splitting the dataset into training and testing groups while making sure that there are equal numbers of attacks and normal activities in each group. Also, testing the suggested model in real-world AIoT settings like edge devices or smart cities could give us a lot of information about how

well it works and how well it can grow. Also, the conclusions of this study would be even more important if they were confirmed through experimental research using different datasets related to intrusion detection. In the end, better models could be made to better forecast network threats by combining AI techniques that are easy to understand and designed for AIoT devices.

References

1. Adhicandra, I.; Tanwir, T.; Asfahani, A.; Sitopu, J.W.; Irawan, F. Latest innovations in Internet of Things (IoT): Digital transformation across industries. Innov. J. Soc. Sci. Res. 2024, 4, 1027–1037.
2. Baranitharan, B.; Prabhkar, G.; Chandran, K.; Vairavel, D.K.; Murugesan, R.; Gheisari, M. Revolutionizing agriculture: A comprehensive review of IoT farming technologies. Recent Adv. Comput. Sci. Commun. 2024, 17, 1–13.
3. Erasto Muwanga, K.; Muwanguzi, E. End user security using smart devices with ability to access IoT services. Int. J. Innov. Sci. Res. Technol. (IJISRT) 2024, 9, 2805–2810.
4. Tawffaq, M.R.; Jasim, M.A.; Mejbel, B.G.; Issa, S.S.; Alamro, L.; Shulha, V.; Aram, E. IoT Security in a Connected World: Analyzing Threats, Vulnerabilities, and Mitigation Strategies. In Proceedings of the 36th Conference of Open Innovations Association (FRUCT), Helsinki, Finland, 30 October–1 November 2024; pp. 626–638.
5. Han, W.; Peng, J.; Yu, J.; Kang, J.; Lu, J.; Niyato, D. Heterogeneous data-aware federated learning for intrusion detection systems via Meta-sampling in artificial intelligence of things. IEEE Internet Things J. 2024, 11, 13340–13354.
6. Dangwal, G.; Wazid, M.; Nizam, S.; Chamola, V.; Das, A.K. Automotive cybersecurity scheme for intrusion detection in can-driven artificial intelligence of things. Secur. Priv. 2024, 8, e483.
7. Stanko, A.; Duda, O.; Mykytyshyn, A.; Totosko, O.; Koroliuk, R. Artificial intelligence of things (AIoT): Integration challenges, and security issues. In Proceedings of the BAIT'2024: The 1st International Workshop on "Bioinformatics and Applied Information Technologies", Zboriv, Ukraine, 2–4 October 2024.
8. Altulaihan, E.; Almaiah, M.A.; Aljughaiman, A. Anomaly detection IDs for detecting DoS attacks in IoT networks based on machine learning algorithms. Sensors 2024, 24, 713.
9. Krishna Prasanth Brahmaji, K. Edge computing and analytics for IoT devices: Enhancing real-time decision making in smart environments. Int. J. Multidiscip. Res. 2024, 6.
10. Rajasekar, P.; Bhosale, R.S.; Indhumathi, C.; Sandeep, K.V.; Rajendiran, M. Real-time Stream Processing in IoT Environments. In Proceedings of the Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Chennai, India, 4–5 April 2024; pp. 1–5.
11. Ameloot, T.; Rogier, H.; Van Torre, P.; Moeneclaey, M. Balancing computational efficiency and detection accuracy in oversampled frequency-shift chirp modulation. IEEE Internet Things J. 2024, 11, 14216–14227.
12. Quincozes, V.E.; Quincozes, S.E.; Albuquerque, C.; Passos, D.G.; Massé, D. Efficient Feature Selection for Intrusion Detection Systems with Priority Queue-Based GRASP. In Proceedings of the IEEE 13th International Conference on Cloud Networking (CloudNet), Rio de Janeiro, Brazil, 27–29 November 2024; pp. 1–8.
13. Bhandari, S.; Kukreja, A.K.; Lazar, A.; Sim, A.; Wu, K. Feature Selection Improves Tree-based Classification for Wireless Intrusion Detection. In Proceedings of the 3rd International Workshop on Systems and Network Telemetry and Analytics, Stockholm, Sweden, 23 June 2020.
14. Musthafa, M.B.; Huda, S.; Kodera, Y.; Ali, M.A.; Araki, S.; Mwaura, J.; Nogami, Y. Optimizing IoT intrusion detection using balanced class distribution, feature selection, and ensemble machine learning techniques. Sensors 2024, 24, 4293.
15. Nazifi Kagara, B. Comparative study on feature selection techniques in intrusion detection systems using ensemble classifiers. Int. J. Innov. Comput. 2021, 11, 27–33.
16. Shukla, S.; Singh, J.; Ramya, T.; Rahul, S.; Mallick, A.K.; Pandey, P. Enhancing Cloud Computing Security through Deep Learning and Attention Mechanism Intrusion Detection Systems. In Proceedings of the 4th International Conference on Intelligent Technologies (CONIT), Bangalore, India, 21–23 June 2024; pp. 1–5.
17. Idouglid, L.; Tkatek, S.; Elfayq, K.; Guezzaz, A. Next-gen security in IIoT: Integrating intrusion detection systems with machine learning for industry 4.0 resilience. Int. J. Electr. Comput. Eng. (IJECE) 2024, 14, 3512–3521.
18. Chandana Swathi, G.; Kishor Kumar, G.; Siva Kumar, A.P. ECBoA-OFS: An ensemble classification model for botnet attacks based on optimal feature selection using CPR in IoT. J. Mach. Comput. 2024, 4, 870–885.
19. Almohaimeed, M.; Albalwy, F. Enhancing IoT network security using feature selection for intrusion detection systems. Appl. Sci. 2024, 14, 11966.
20. Shu, X.; Ye, Y. Knowledge discovery: Methods from data mining and machine learning. Soc. Sci. Res. 2023, 110, 102817. [PubMed]
21. Soltani, M.; Khajavi, K.; Jafari Siavoshani, M.; Jahangir, A.H. A multi-agent adaptive deep learning framework for online intrusion detection. Cybersecurity 2024, 7, 9.
22. Sajid, M.; Malik, K.R.; Almogren, A.; Malik, T.S.; Khan, A.H.; Tanveer, J.; Rehman, A.U. Enhancing intrusion detection: A hybrid machine and deep learning approach. J. Cloud Comput. 2024, 13, 123.

23. Kanna, P.R.; Santhi, P. Unified deep learning approach for efficient intrusion detection system using integrated spatial–temporal features. Knowl.-Based Syst. 2021, 226, 107132.
24. Henry, A.; Gautam, S.; Khanna, S.; Rabie, K.; Shongwe, T.; Bhattacharya, P.; Sharma, B.; Chowdhury, S. Composition of hybrid deep learning model and feature optimization for intrusion detection system. Sensors 2023, 23, 890.
25. Dina, A.S.; Siddique, A.; Manivannan, D. A deep learning approach for intrusion detection in Internet of Things using focal loss function. Internet Things 2023, 22, 100699.
26. Awad, A.A.; Ali, A.F.; Gaber, T. An improved long short term memory network for intrusion detection. PLoS ONE 2023, 18, e0284795.
27. Shaji, N.S.; Jain, T.; Muthalagu, R.; Pawar, P.M. Deep-discovery: Anomaly discovery in software-defined networks using artificial neural networks. Comput. Secur. 2023, 132, 103320.
28. Nguyen, D.-T.; Le, K.-H. The robust scheme for intrusion detection system in internet of things. Internet Things 2023, 24, 100999.
29. Chen, Y.; Zhao, C. Application of deep learning model in computer data mining intrusion detection. Appl. Math. Nonlinear Sci. 2023, 8, 2131–2140.
30. Wang, X.; Wang, Y.; Javaheri, Z.; Almutairi, L.; Moghadamnejad, N.; Younes, O.S. Federated deep learning for anomaly detection in the internet of things. Comput. Electr. Eng. 2023, 108, 108651.
31. Saba, T.; Rehman, A.; Sadad, T.; Kolivand, H.; Bahaj, S.A. Anomaly-based intrusion detection system for IoT networks through deep learning model. Comput. Electr. Eng. 2022, 99, 107810.
32. Abusitta, A.; de Carvalho, G.H.; Wahab, O.A.; Halabi, T.; Fung, B.C.; Al Mamoori, S. Deep learning-enabled anomaly detection for IoT systems. Internet Things 2023, 21, 100656.
33. Abdelmoumin, G.; Rawat, D.B.; Rahman, A. On the performance of machine learning models for anomaly-based intelligent intrusion detection systems for the internet of things. IEEE Internet Things J. 2021, 9, 4280–4290.
34. Ullah, I.; Mahmoud, Q.H. Design and development of RNN anomaly detection model for IoT networks. IEEE Access 2022, 10, 62722–62750.
35. Jia, Y.; Lin, F.; Sun, Y. A novel federated learning aggregation algorithm for AIoT intrusion detection. IET Commun. 2024, 18, 429–436.
36. Ferrag, M.A.; Friha, O.; Hamouda, D.; Maglaras, L.; Janicke, H. Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. IEEE Access 2022, 10, 40281–40306.
37. Zegarra Rodriguez, D.; Daniel Okey, O.; Maidin, S.S.; Umoren Udo, E.; Kleinschmidt, J.H. Attentive transformer deep learning algorithm for intrusion detection on IoT systems using automatic Xplainable feature selection. PLoS ONE 2023, 18, e0286652.
38. Sharmila, B.S.; Nagapadma, R. RT-IoT2022; UC Irvine Machine Learning Repository: Irvine, CA, USA, 2023.
39. Sharmila, B.; Nagapadma, R. Quantized autoencoder (QAE) intrusion detection system for anomaly detection in resourceconstrained IoT devices using RT-IoT2022 dataset. Cybersecurity 2023, 6, 41.
40. Bharadiya, J.P. The role of machine learning in transforming business intelligence. Int. J. Comput. Artif. Intell. 2023, 4, 16–24.
41. Pande, S.; Khamparia, A.; Gupta, D. Feature selection and comparison of classification algorithms for wireless sensor networks. J. Ambient Intell. Humaniz. Comput. 2023, 14, 1977–1989.
42. Moslemi, A. A tutorial-based survey on feature selection: Recent advancements on feature selection. Eng. Appl. Artif. Intell. 2023, 126, 107136.
43. Masoudi-Sobhanzadeh, Y.; Motieghader, H.; Masoudi-Nejad, A. FeatureSelect: A software for feature selection based on machine learning approaches. BMC Bioinform. 2019, 20, 170.
44. Abdi, H.; Williams, L.J. Principal component analysis. Wiley Interdiscip. Rev. Comput. Stat. 2010, 2, 433–459.
45. Zou, J.; Han, Y.; So, S.-S. Overview of artificial neural networks. In Artificial Neural Networks: Methods And Applications; Humana Press: Totowa, NJ, USA, 2009; pp. 14–22.
46. Arik, S.Ö.; Pfister, T. abnet: Attentive Interpretable Tabular Learning. In Proceedings of the AAAI Conference on Artificial Intelligence, Online, 2–9 February 2021; pp. 6679–6687.
47. Hwang, Y.; Song, J. Recent deep learning methods for tabular data. Commun. Stat. Appl. Methods 2023, 30, 215–226.
48. Otokwala, U.; Petrovski, A.; Kalutarage, H. Optimized common features selection and deep-autoencoder (OCFSDA) for lightweight intrusion detection in Internet of Things. Int. J. Inf. Secur. 2024, 23, 2559–2581.

49. Gaur, V.; Kumar, R. Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices. Arab. J. Sci. Eng. 2022, 47, 1353–1374.
50. Chen, Y.; Li, J.; Guo, N. Efficient and interpretable SRU combined with TabNet for network intrusion detection in the big data environment. Int. J. Inf. Secur. 2023, 22, 679–689.
51. Muruganandam, S.; Joshi, R.; Suresh, P.; Balakrishna, N.; Kishore, K.H.; Manikanthan, S. A deep learning based feed forward artificial neural network to predict the K-barriers for intrusion detection using a wireless sensor network. Meas. Sens. 2023, 25, 100613.
52. Sharma, B.; Sharma, L.; Lal, C. Anomaly-Based DNN Model for Intrusion Detection in IoT and Model Explanation. In Proceedings of the Second International Conference on Computational Electronics for Wireless Communications, Surathkal, India, 9–10 June 2022; Springer: Singapore, 2023.
53. Chen, R.-C.; Dewi, C.; Huang, S.-W.; Caraka, R.E. Selecting critical features for data classification based on machine learning methods. J. Big Data 2020, 7, 52.