JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

ENHANCING IOT SECURITY THROUGH MACHINE LEARNING-BASED INTRUSION DETECTION SYSTEMS

[1]Prof. Monali B Suthar, [2]Dr. Satvik Khara
[1] Assistant Professor, [2] Head of Computer Engineering
Department of Computer Engineering,
Silver Oak College of Engineering and Technology
Silver Oak University

Abstract : The rapid proliferation of Internet of Things (IoT) devices has introduced numerous benefits across various domains, ranging from healthcare to smart homes and industrial automation. However, the interconnected nature of IoT devices also brings forth significant security challenges, particularly regarding the detection and prevention of intrusions. Traditional intrusion detection systems (IDS) struggle to cope with the unique characteristics and constraints of IoT environments[1]. This research paper explores the application of machine learning (ML) approaches for intrusion detection in IoT networks. We discuss the challenges associated with securing IoT systems, review existing research on intrusion detection in IoT [2][3], and evaluate the effectiveness of machine learning techniques in mitigating IoT security threats [4][5]. Through a comprehensive analysis of the literature, we identify key trends, methodologies, and areas for future research in the domain of intrusion detection in IoT using machine learning.

Keywords : IoT, Intrusion Detection, Machine Learning, Security, Cybersecurity, Supervised Learning, Unsupervised Learning, Deep Learning.

I. INTRODUCTION :

The Internet of Things (IoT) has emerged as a transformative paradigm, revolutionizing the way we interact with technology and shaping the landscape of various industries including healthcare, transportation, agriculture, and smart cities [1]. By interconnecting a vast array of devices and sensors, IoT facilitates seamless data exchange and enables the automation of processes, leading to increased efficiency, productivity, and convenience[3]. However, this unprecedented connectivity also introduces a myriad of security challenges, with IoT devices becoming prime targets for malicious actors seeking to exploit vulnerabilities and compromise the integrity of systems[5].

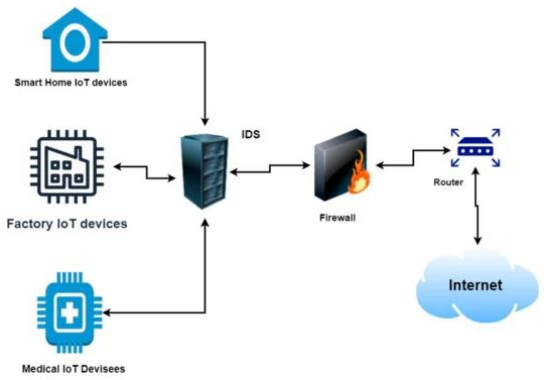

Figure 1.1 Network Architecture for IoT.

Securing IoT ecosystems poses unique and complex challenges due to the heterogeneity of devices, resource constraints, scale, dynamic nature, lack of standardization, and privacy concerns inherent in these environments [2]. Traditional security mechanisms are often inadequate to address these challenges effectively, necessitating the development of novel approaches tailored specifically for IoT environments [4]. Among these approaches, intrusion detection systems (IDS) play a critical role in safeguarding IoT networks by detecting and mitigating security breaches in real-time [6].

In recent years, there has been a growing interest in leveraging machine learning (ML) techniques for intrusion detection in IoT environments [1]. Machine learning offers the potential to enhance the effectiveness of intrusion detection systems by enabling them to adapt to evolving threats, identify anomalous behaviour, and distinguish between legitimate and malicious activities with high accuracy[3]. This research paper aims to explore the machine learning approaches for intrusion detection in IoT networks.

This paper will provide an overview of the security challenges inherent in IoT environments, highlighting the unique characteristics and constraints that influence intrusion detection. Review existing research literature on intrusion detection in IoT, focusing on both traditional and machine learning-based approaches. Evaluate the effectiveness of machine learning deep learning techniques in addressing IoT security threats, considering factors such as performance, scalability, energy efficiency, and real-time detection capabilities. Discuss dataset considerations, evaluation metrics, and experimental methodologies relevant to intrusion detection in IoT using machine learning[9].

II. OBJECTIVE :

The objective of conducting intrusion detection in IoT using a machine learning approach, specifically employing Deep Neural Networks (DNNs), is to enhance the security posture of IoT ecosystems by effectively identifying and mitigating potential security breaches and malicious activities [2]. The specific goals of this research endeavour are outlined as follows:

Develop Effective Intrusion Detection Mechanisms: Design and implement intrusion detection systems tailored for IoT environments that leverage the capabilities of machine learning algorithms, particularly DNNs, to accurately detect anomalous behaviour and security threats[4].

Enhance Detection Accuracy: Improve the accuracy and efficacy of intrusion detection in IoT networks by harnessing the representational power and hierarchical feature learning capabilities of DNNs, enabling the system to distinguish between normal and malicious network behaviour with high precision [5].

Address IoT-Specific Challenges: Identify and address the unique challenges associated with intrusion detection in IoT systems, including the heterogeneity of devices, resource constraints, dynamic network topology, and diverse communication protocols, by devising machine learning-based solutions that are adaptable and scalable [7].

Explore Feature Representation: Investigate effective feature representation techniques for capturing the complex patterns and characteristics of IoT network traffic, ensuring that the intrusion detection system can effectively discern between benign and malicious activities across various IoT device types and communication protocols [9].

Optimize Resource Utilization: Develop intrusion detection models that are resource-efficient and suitable for deployment on resource-constrained IoT devices, considering factors such as computational complexity, memory footprint, and energy consumption, to minimize overhead and maximize scalability [3].

Evaluate Performance and Robustness: Conduct rigorous performance evaluation and robustness testing of the proposed intrusion detection system using diverse datasets and realistic IoT network scenarios, assessing metrics such as detection accuracy, false positive rate, detection latency, and resilience to adversarial attacks [5].

Facilitate Real-Time Detection: Enable real-time intrusion detection capabilities within IoT networks by developing efficient inference algorithms and deployment strategies that allow the intrusion detection system to operate autonomously and promptly respond to security threats as they arise [7].

Inform Security Policy Enforcement: Provide actionable insights and recommendations to IoT system administrators and security practitioners based on the detected security incidents and anomalies, enabling proactive security policy enforcement and threat mitigation measures to safeguard IoT deployments effectively [8].

III. LITERATURE SURVEY

Several scientific articles have been published on IDS that used data mining and ML techniques. The advent of the Internet of Things (IoT) has revolutionized how devices interact within various ecosystems, creating a vast network of interconnected devices. However, the exponential growth of IoT devices has also led to significant security challenges, making Intrusion Detection Systems (IDS) a critical area of research. This literature survey explores recent advancements in IDS for IoT environments, focusing on the integration of machine learning techniques to enhance detection capabilities.

3.1. Machine Learning Approaches in IDS

The application of machine learning techniques in IDS has gained significant attention due to their ability to adapt to evolving threats and complex network environments. This algorithm in [4]was evaluated using the BoT-IoT dataset, and the results demonstrated superior performance compared to traditional methods. This study underscores the potential of deep learning in enhancing the security of IoT networks [4].

Another important contribution in this domain is the development of a comprehensive security framework that integrates multiple advanced technologies, including Software Defined Networking (SDN), Network Function Virtualization (NFV), and machine learning. in [5] framework aims to create a holistic security solution capable of autonomously adapting to emerging IoT threats that do not follow known patterns or signatures. The integration of these technologies within a unified framework represents a significant advancement in the field of IoT security [5].

Several studies highlight the critical role of feature selection in improving the performance of ML algorithms. Gupta et al. (2021) proposed a genetic algorithm-based feature selection method that enhanced the accuracy of classifiers like Decision Trees and Support Vector Machines (SVM) (Gupta et al., 2021).While effective, feature selection methods can be computationally intensive and may still miss relevant features, especially in dynamic IoT environments where device behaviour evolves over time.[16]

Anomaly-based intrusion detection systems (IDS) are effective in identifying unusual patterns. Ahmed et al. (2020) developed a model using k-Nearest Neighbours (k-NN) and Random Forests, achieving high detection rates on various datasets (Ahmed et al., 2020). Anomaly detection can suffer from high false positive rates, particularly in environments with legitimate but variable behaviour, leading to alert fatigue among security personnel[17].

Khan et al. (2021) created a hybrid IDS using SVM and clustering algorithms, demonstrating enhanced accuracy and reduced false positives (Khan et al., 2021). The complexity of hybrid models can lead to longer training times and may require extensive tuning to achieve optimal performance[18].

Shatnawi et al. (2022) employed a deep autoencoder architecture to identify anomalies in IoT environments, effectively reconstructing normal patterns (Shatnawi et al., 2022). The performance of autoencoders can degrade in the presence of noisy data or when the distribution of normal data changes significantly over time.[19]

3.2. Comparative Analysis of Datasets

The comparative analysis of different datasets and methodologies is crucial for understanding the strengths and limitations of various IDS approaches. The UNSW-NB15 dataset, for instance, has been widely adopted due to its comprehensive nature, which includes a broad range of attack types and realistic traffic patterns. On the other

hand, the KDD Cup 1999 dataset, despite being older, remains a popular benchmark due to its extensive use in early IDS research. Studies comparing feature selection methods on these datasets have highlighted the importance of choosing appropriate features to enhance detection accuracy while reducing computational costs [2].

As IoT networks continue to grow and evolve, the need for adaptive and robust IDS will become increasingly critical. Future research should focus on developing more sophisticated machine learning models that can detect previously unknown attack patterns and autonomously update themselves to respond to emerging threats. Additionally, the continuous improvement of datasets like UNSW-NB15 and the creation of new benchmarks that reflect the latest advancements in network traffic and attack methodologies will be essential for advancing IDS research[6].

The integration of machine learning techniques into IDS for IoT networks has shown significant promise in improving detection accuracy and efficiency. The development of comprehensive datasets like UNSW-NB15, combined with advanced feature selection methods and deep learning approaches, has enabled researchers to create more robust and effective IDS. However, as the IoT landscape continues to evolve, ongoing research and innovation will be required to keep pace with the increasing complexity and sophistication of cyber threats[8].

IV. Dataset and Feature Selection

One of the major challenges in developing effective IDS is the unavailability of comprehensive and realistic benchmark datasets that accurately reflect modern network traffic. The UNSW-NB15 dataset, created by the University of New South Wales, addresses this gap by offering a hybrid dataset that includes both real-world normal activities and synthesized attack scenarios. UNSW-NB15 dominates the defects of the KDD99 dataset (for instance, no modern attacks, etc.) and has inchmeal become the most favourite dataset in the area of IoT intrusion detection in recent years. This dataset has become a crucial resource for evaluating IDS performance, particularly in IoT environments. Researchers have utilized machine learning techniques to analyse the features within this dataset, focusing on overcoming the "curse of high dimensionality" to enhance intrusion detection accuracy [1].

Statistical features		16 hours	15 hours
No._of_flows		987,627	976,882
Src_bytes		4,860,168,866	5,940,523,728
Des_bytes		44,743,560,943	44,303,195,509
Src_Pkts		41,168,425	41,129,810
Dst_pkts		53,402,915	52,585,462
Protocol types	TCP	771,488	720,665
	UDP	301,528	688,616
	ICMP	150	374
	Other	150	374
Label	Normal	1,064,987	1,153,774
	Attack	22,215	299,068
Unique	Src_ip	40	41
	Dst_ip	44	45

Table 4.1. DATA SET STATISTICS

The 9 types of attack categories are namely Analysis, Fuzzers, Exploits, Shellcode, Reconnaissance, DOS, Backdoors, Shellcode, and Worms of UNSW-NB15 Training Dataset and as represented by the graph in (Figure 4.1).

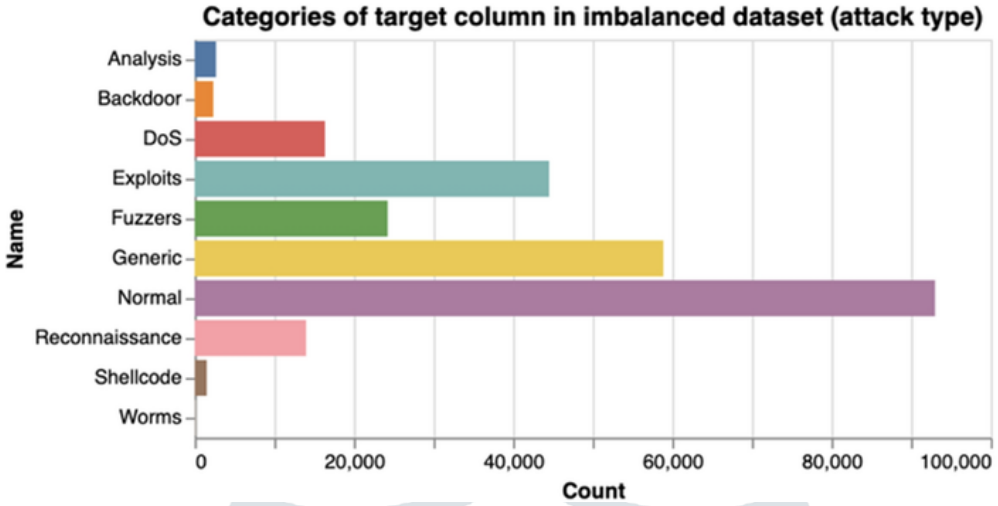

Figure 4.1. DATA SET STATISTICS

Feature selection plays a critical role in optimizing IDS performance. By employing techniques such as Information Gain (IG) and Gain Ratio (GR), researchers have been able to identify the most relevant features for detecting specific types of attacks, such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. [3]. In [13] they have only top 4 features of the UNSW-NB15 Dataset that are extracted from the total 45 features by using the combination fusion algorithm of RandomForest algorithm and Decision tree classifier.

V. PROPOSED METHOD:

The proposed DCNN algorithm with Neighbourhood Search Based Particle Swarm Optimization , is an enhancement of the traditional Particle Swarm Optimization (PSO) algorithm. It integrates concepts from the Artificial Bee Colony (ABC) algorithm and leverages the feature extraction power of Deep Convolutional Neural Networks (DCNNs) to improve exploration, exploitation, and solution representation capabilities on the UNSW NB 15 dataset.

PSO is a meta-heuristic optimization algorithm inspired by the social behaviour of birds flocking or fish schooling. In PSO, a population of candidate solutions, called particles, moves through the search space to find the optimal solution. Each particle adjusts its position based on its own experience (local best) and the experience of its neighbours (global best).

In the proposed algorithm, multiple particles, referred to as employed bees, represent the global best solutions at any given time. By considering these employed bees, different regions of the search space can be explored simultaneously. This multi-directional search helps in avoiding the common problem of being trapped in local minima, which is a limitation of traditional PSO.

The algorithm further integrates the ABC algorithm's mechanism, where onlooker bees are introduced to exploit the vicinity of the employed bees. The role of these onlooker bees is to perform a neighbourhood search around the employed bees. If an onlooker bee finds a better solution than its corresponding employed bee, it replaces the employed bee, thereby updating the employed bee's position. Figure 5.1 indicates an overview of particle velocity motions in the PSO algorithm.

Equations (1) and (2) represent the velocity and position of the particles, respectively.

$$V_{id}(t+1)=\alpha V_{id}(t)+\beta \text{rand}(0,\varphi_1)(P_{id}(t)-X_{id}(t))+\beta \text{rand}(0,\varphi_2)(P_{gd}(t)-X_{id}(t)) \quad (5.1)$$

$$X_{id}(t+1)=X_{id}(t)+V_{id}(t+1) \quad (5.2)$$

where V_{id}(t)= the current velocity of particle in dimension, d, V_{id}(t+1) = the new velocity of particle in dimension, d, X_{id}(t) = the current position of particle in dimension, d, X_{id}(t+1) = the new position of particle in dimension d; βrand(0,φ_1) = a random number between zero and φ_1, βrand(0,φ_2) = a random number between zero and φ_2, α = the inertial coefficient, $P_{id}(t)$ = the best personal experience of particles in dimension d ,and $P_{gd}(t)$ = the best global experience of particles in dimension d

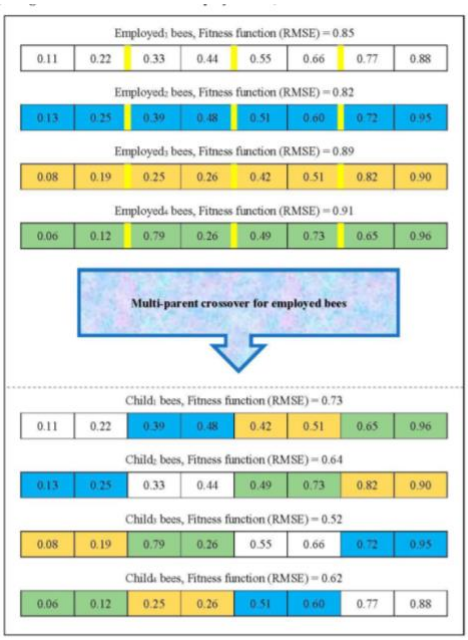

Figure 5.1 The example of a neighbourhood search around employed bees

Once the onlooker bees complete their search and the employed bees are updated, the algorithm compares the newly updated employed bees to the current global best solution. If any of these updated employed bees provide a better solution than the current global best, the global best is also updated accordingly.

In standard PSO, the particle diversity gradually decreases as the particles move towards the personal best and global best. In this paper, due to the exploratory nature of the crossover operator, a multi-parent crossover is proposed to achieve highly varied solutions. In this operator, instead of using two employed bees, all employed bees participate in the crossover to create new solutions. When we use several best particles (as employed bees) to produce the new solutions, the obtained child bears less similarity to its parent, meaning that the solutions are diverse in the search space. Therefore, the multi-parent crossover operator improves the algorithm exploration. Figure 5.2 shows the example of the multi-parent crossover operator of the proposed algorithm.

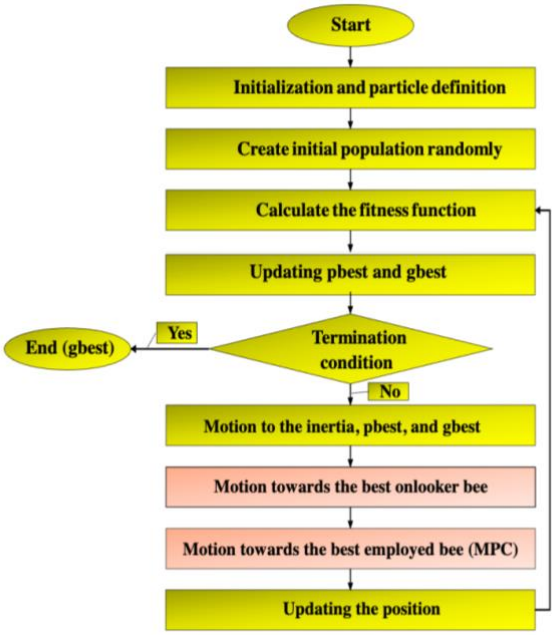

Figure 5.2 Flowchart of algorithm

This algorithm enhances the traditional PSO by incorporating the neighbourhood search and update mechanisms from the ABC algorithm, resulting in a more robust and effective optimization process. This hybrid approach leverages the strengths of both PSO and ABC, making it well-suited for complex optimization problems where the search space is large and the risk of local minima is significant. Therefore, Equation (1) is updated as follows and two new vectors are added to improve the PSO performance .

$$V_{id}(t+1)=\alpha V_{id}(t)+\beta rand(0,\varphi_1)(P_{id}(t)-X_{id}(t))+\beta rand(0,\varphi_2)(P_{gd}(t)-X_{id}(t))+\beta rand(0,\varphi_3)(P_{od}(t)-X_{id}(t))+\beta rand(0,\varphi_4)(P_{ed}(t)-X_{id}(t)) \quad (5.3)$$

Feature Extraction: A Deep Convolutional Neural Network (DCNN) is employed to extract high-level features from the input data. These features are then used to represent the particles in the PSO algorithm, providing a more informed and structured search space.

Particle Representation: The particles in the PSO algorithm are not just simple vectors but are represented by the deep features extracted by the DCNN, which encapsulates the most relevant information from the data.

Enhanced Search: By using deep features, the algorithm can perform more sophisticated searches, leveraging the hierarchical representation of data to navigate complex solution landscapes effectively.

The algorithm iteratively repeats the process of neighbourhood search, updating employed bees, refining the global best, and enhancing the feature representation through the DCNN until a termination condition is met. The overall schematic of the proposed classifier is depicted in Figure 5.3. According to this figure, the input data passes through some convolution and pooling layers. After that, we use a fully connected MLP to classify the datasets. The fully connected MLP is trained by the proposed in order to achieve a higher classification and detection rate. Figure 5.3 shows the flowchart of the proposed algorithm.

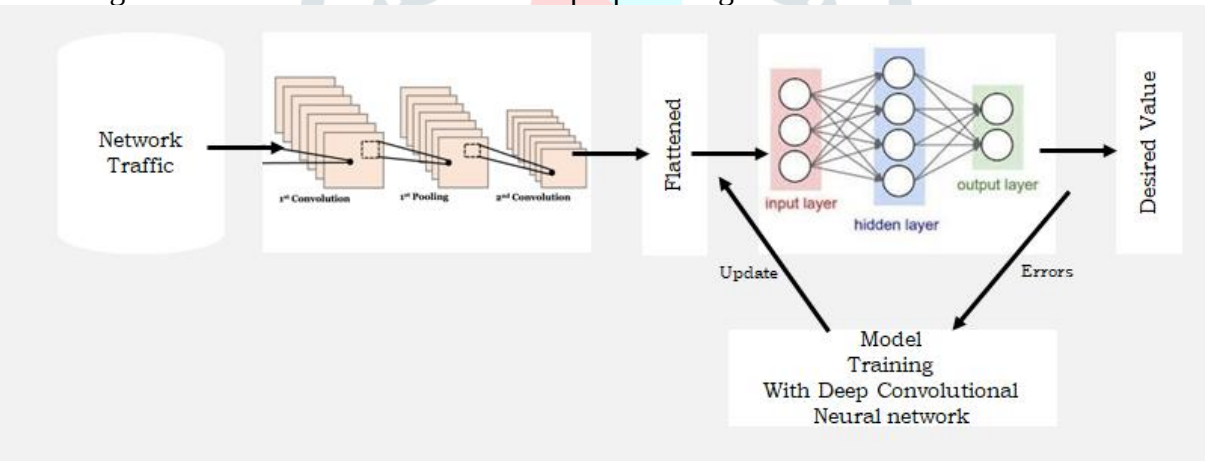

Figure 5.3 Overall Flow Chart of deep learning algorithm

The fitness function of the proposed approach can be calculated as Equation

$$\text{Mean Square Error (MSE)} = \frac{1}{k}\sum_{i=1}^{k}(Oi - Di)^2 \quad (5.4).$$

where, k = the total number of samples, O_i = system output, and D_i = desire.

For validation, accuracy metrics are used to compare the performance of the deep architectures.

VI. RESULTS AND DISCUSSION :

Intrusion detection particularly in IoT has been explored remarkably over the years by the research community. The vulnerability that exists in IoT devices especially because of the large amount of data that transmit from one IoT node to another has been a major concern. Hence to handle this issue, several machine

learning approaches have been proposed but the results are not as convincing, as it indicates a high complexity in the feature extraction process. Eventually, a better option is proposed involving the use of deep learning approaches to design a more robust anomaly detection algorithm.

The proposed algorithm significantly outperforms all other methods tested, with an accuracy of 99.41%. This highlights the effectiveness of the hybrid approach that combines optimization and deep learning techniques to handle complex data sets. Traditional methods like CNN, RNN, and combinations like LSTM+CNN or PCA+CNN perform well but do not reach the high level of accuracy achieved by the proposed algorithm. The poor performance of autoencoders further emphasizes the necessity of integrated and advanced strategies for optimal results in network intrusion detection and similar tasks.

Algorithm	Accuracy
Proposed	99.41
CNN	97.55
RNN	97.00
Autoencoders	31.00
LSTM+CNN	96.75
PCA+CNN	96.97
SVD+CNN	97.04

Table 6.1 Accuracy % table of deep learning algorithms

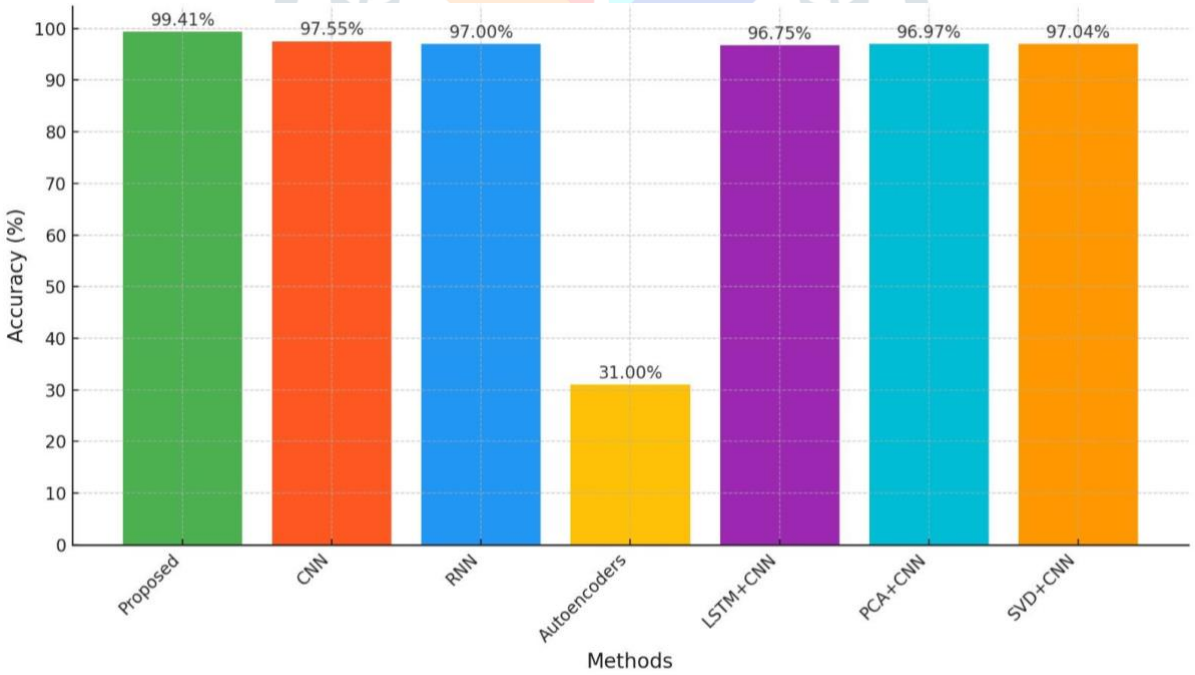

Figure 6.1 Accuracy bar chart of deep learning algorithm

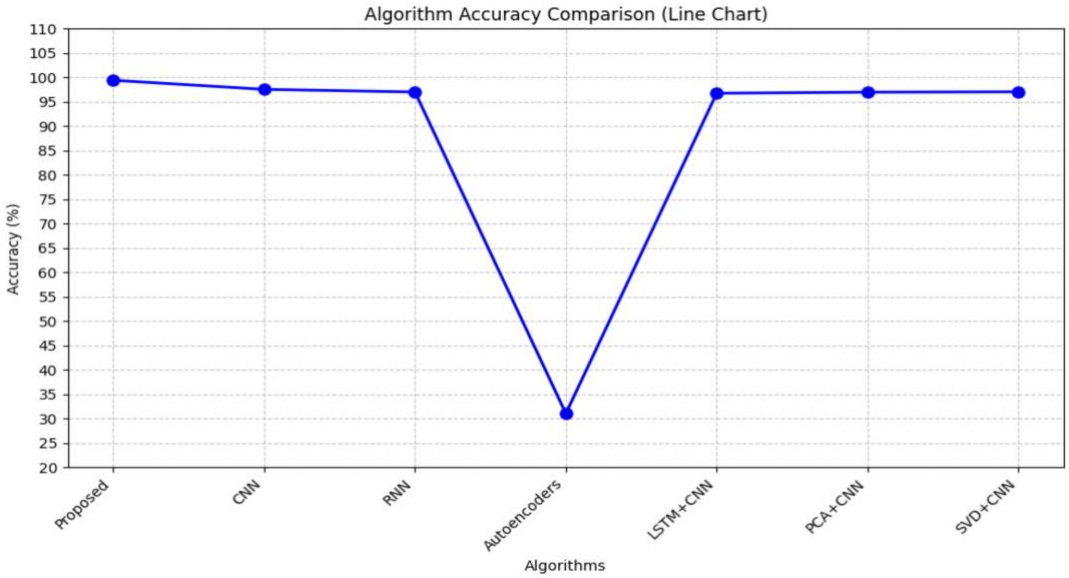

Figure 6.2 Accuracy line chart of deep learning algorithm

The proposed algorithm represents a significant advancement in the field of optimization by combining the strengths of Particle Swarm Optimization (PSO), Artificial Bee Colony (ABC), and Deep Convolutional Neural Networks (DCNN). By integrating these techniques, the algorithm effectively addresses the challenges of local minima entrapment and high-dimensional data representation, which are common in traditional optimization methods. algorithm provides a powerful and versatile framework for solving optimization problems, offering a blend of traditional meta-heuristic techniques and modern deep learning approaches. Its ability to navigate complex solution landscapes efficiently makes it a promising tool for a wide range of applications.

REFERENCES

1. S. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Dataset for Network Intrusion Detection Systems," IEEE, 2015.
2. A. K. Jain and A. K. Sharma, "Feature Selection in UNSW-NB15 and KDDCUP'99 Datasets," IEEE, 2018.
3. M. S. Chen, H. H. Xu, and X. X. Zheng, "Feature Selection for Intrusion Detection Systems in IoT," Elsevier, Apr. 2021.
4. J. Lee and J. Park, "An Intrusion Detection System Using BoT-IoT," IEEE, Apr. 2023.
5. C. J. Wang and Y. R. Li, "A Machine Learning Security Framework for IoT Systems," IEEE, 2020.
6. Fatima Hussain, Rasheed Hussain, Syed Ali Hassan, and Ekram Hossain "Machine Learning in IoT Security: Current Solutions and Future Challenges" IEEE April 2020.
7. miloud bagaa, tarik taleb, jorge bernal bernabe and antonio skarmeta "A Machine Learning Security Framework for IoT Systems" IEEE Access IEEE 2020
8. A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2020.
9. Nickson M. Karie, Nor Masri Sahri, Paul Haskell-Dowland "IoT Threat Detection Advances, Challenges and Future Directions.", May 27,2020 ,IEEE.
10. Arunan Sivanathan , Hassan Habibi Gharakheili , and Vijay Sivarama "Managing IoT Cyber-Security Using Programmable Telemetry and Machine Learning" Ieee Transactions On Network And Service Management, Vol. 17, No. 1, March 2020
11. Bruno Bogaz, ZarpelãoaRodrigo, SanchesMianibCláudio, ToshioKawakaniaSean, Carlistode Alvarengaa"A survey of intrusion detection in Internet of Things" Volume 84, 15 April 2017, Pages 25-37
12. Lirim Ashiku,Cihan Dagli,"Network Intrusion Detection System using Deep Learning",Elsevier B.V. 2021
13. V. Kanimozhi, Prem Jacob,"UNSW-NB15 Dataset Feature Selection and Network Intrusion Detection using Deep Learning",International Journal of Recent Technology and Engineering,Volume-7 Issue-5S2, January 2019
14. Hanif, S.; Ilyas, T.; Zeeshan, M. Intrusion detection in IoT using artificial neural networks on UNSW-15 dataset. In Proceedings of the 2019 IEEE 16th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT and AI (HONET-ICT), Charlotte, NC, USA, 6–9 October 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 152–156
15. 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
16. Gupta, A., et al. (2021). A novel feature selection and classification approach for IoT intrusion detection. IEEE Access, 9, 34656-34668.
17. Ahmed, M., Mahmood, A. N., & Hu, J. (2020). A survey of network anomaly detection systems using machine learning techniques. Journal of Network and Computer Applications, 151, 102492.
18. Khan, M. A., et al. (2021). A hybrid machine learning model for intrusion detection in IoT networks. Journal of Ambient Intelligence and Humanized Computing, 12(3), 3075-3086.
19. Shatnawi, A. M., et al. (2022). Deep learning-based anomaly detection for IoT systems using autoencoders. IEEE Transactions on Network and Service Management, 19(2), 1155-1167.