SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V11I3P116

Volume 11 Issue 3, 201-208, March 2024

Original Article

Using Optimized Artificial Intelligence Techniques to Prevent Cyber Security with the Internet of Things

Vidya Sivalingam[1], Shabana Parveen[2], Rubeena[3], Jayasuriya Panchalingam[4]

[1]*Department of Information Technology and Security, College of Computer Science and Information Technology, Jazan University, Jazan, Saudi Arabia.*
[2,3,4]*Department of Computer Science, College of Computer Science and Information Technology, Jazan University, Jazan, Saudi Arabia.*

[1]*Corresponding Author : vidyakomaghanresearch@gmail.com*

Received: 11 January 2024 Revised: 08 February 2024 Accepted: 09 March 2024 Published: 25 March 2024

Abstract *- The Internet of Things (IoT) provides high levels of security for physical items like smart appliances and household appliances. The Internet Protocol (IP) gives each physical item a distinct online address that it may use to communicate with other devices on the network and the outside world via the internet. As the number of hacker attacks on data transmission over the internet continues to climb, there is a growing concern about cybersecurity vulnerabilities in IoT devices. To construct a reliable Cyber Security (CS) system in the face of such potent attacks, attack detection is essential. Common threats to IoT systems include data-type probing, Denial-of-Service (DoS), and User-to-Root (U2R) attacks. Unfortunately, current methods for detecting and investigating IoT malware are insufficient. DoS attacks occur in IoT settings due to inadequate security monitoring and preventive actions. In order to predict attacks as well as problems with IoT devices, this article examines a number of performance-based Artificial Intelligence (AI) algorithms. Several improved optimisation approaches, particularly particle swarm optimisation techniques, were used to determine the productivity of the proposed AI strategy in detail for four different parameters. Hence, this article combines a machine learning method with an optimization algorithm to perform efficient feature extraction. The proposed method's efficiency is shown by relating its outcomes to those of the existing systems.*

Keywords *- Cyber Security, AI, Deep Learning (DL), IoT, Optimization.*

1. Introduction

An IoT is a decentralised network that uses wired and wireless communication technologies to link various sensor systems and devices, barcodes, QR codes, global positioning systems, RFID readers, and more to the internet. Because of this, embedded systems can link up and exchange data with one another [1]. In up-to-date centuries, the usage of the IoT has advanced exponentially, and with it, the prevalence of CS threats. Intricate algorithms that protect networks and systems, including IoT systems, are being developed using AI at the forefront of CS [2].

One of the crucial technologies for modern smart CS systems or rules is DL, derived from Artificial Neural Networks (ANNs). The aids and problems of AI in cyber risk analytics include its ability to increase organisational flexibility as well as our comprehension of cyber risk [3]. Due to its extensive usage, people are starting to worry more and more about the security of the IoT. Paralysed equipment and massive data loss are the results of a hostile attack on an IoT system. Propose the LM-BP neural network to solve the IoT security problem [4]. Adaptable rules, robust privacy protection, and decentralised private blockchains may be used in the industrial IoT to manage massive amounts of data and solve security challenges. But, blockchain's scalability is a limiting factor for IIoT. Because of this, this study proposes a better algorithm based on Two_Arch2 to reduce cost as well as delay in the blockchain while increasing its scalability and decentralisation [5].

This is one area where IoT technologies clash with more conventional forms of security. CS has emerged as a major issue for the IoT and the Industrial IoT, with the goal of lowering end-user and company CS risks. Modern CS software and hardware provide better oversight of the IoT [6].

The study delves deeply into the topic of federated DL methods and their impact on the CS of IoT applications, providing a trial analysis and inquiry. Specifically, an outline of federated learning-rooted security along with privacy systems for various IoT applications, with edge computing, industrial IoT, the internet of drones, the internet of healthcare things, the internet of automobiles, and more [7]. In order to analyse and filter the data, a data-driven approach to

anomalies and ID is proposed. Improving the training dataset's quality is possible using mutual information and the SMOTE algorithm [8]. Though several approaches have been proposed in the existing works to detect security accurately, some issues still remain. The primary issue is the selection of features and the failure of an optimisation algorithm to select the features. In [23], a hybrid use of some optimization algorithms is employed for cybersecurity prevention. However, this work does not use any ML-based approaches to detect attacks efficiently. So, this work makes the following contributions to work with these limitations:

- Initially, pre-processing is done with the dataset to remove the missing values and irrelevant information.
- The main idea behind Feature Selection (FS) is to enhance the predictor's accuracy along with functionality.
- The research study suggests the finest way to develop the presentation of IDSs with the least amount of computer complexity is by grouping together a set of simplified characteristics.
- An optimization algorithm called Particle Swarm Optimization (PSO) was used to improve the performance with FS.
- Therefore, FS is used to reduce irrelevant characteristics and improve the performance of classifiers.
- For classification, this study makes use of the more modern gradient-boosting method called the Catboost classifier. Using a more effective approach to prevent overfitting, Catboost is a novel supervised technique that uses gradient boosting on decision trees to categorise categorical data. To get better results, use the Catboost algorithm with PSO. Hence, the ML algorithm with an optimization algorithm provides accurate detection.
- The NSL-KDD dataset is an adapted form that is used for FS. The proposed approach and the KDD Cup 99 dataset led to increased Intrusion Detection (ID) accuracy.

Generally, in this type of work, mostly only classifiers are used for prediction. However, in this work with the classification phase, the preprocessing phase is added, followed by an efficient feature selection phase. Since feature selection is made through optimization algorithms, other than the normally used classifier, the catboost classifier, which has been efficient recently, is used in this work. Below is the outline for the remainder of the article. Section 2 summarises previous work on the IoT topic using various methods. Section 3 defines the proposed method, while section 4 discusses its outcomes. The references come after section 5, which determines the work.

2. Literature Review

Tomazzoli et al. [9] discuss both business and household use; energy efficiency poses significant difficulties in this regard. In sectors where monitoring the power consumption of distant branches is essential, the scalability of energy management systems presents a unique set of challenges. A system can't be said to be autonomous until it can independently use consumption data to create and implement behavioural rules. To achieve the highest possible level of energy efficiency, it is necessary to establish best practices tailored to the specific energy arrangement. In addition, there has to be an automated system in place to update and apply best practices to topological changes. This article utilises Machine Learning (ML) methods and the IoT paradigm to create a one-of-a-kind system architecture for centralised energy efficiency in dispersed sub-networks of electric appliances. It also uses these approaches to distinguish between different types of devices, remove behavioural rules, and identify the finest output.

Li et al. [10] to get a thorough knowledge of the linkages between these four interrelated domains and how they might be integrated with smart energy management systems. By estimating energy demand, load profiles, and planning resources, AI models provide predictable performance and efficient use of energy resources. Algorithms for AI training need massive data sets. Discoveries made possible by data mining and large data systems dictate how well AI systems work. It is also possible to train AI using ever-more-accurate data thanks to data mining, which improves the collected information.

Mao et al. [11] provided an adaptive security specification technique for these networks based on AI. 6G IoT networks connect IoT devices to cellular networks utilising a range of frequency bands, including Terahertz (THz) along with millimetre wave (mmWave). IoT sensing devices may lend a hand to the energy harvesting method, which is projected to see extensive use in 6G. The proposal first employs the Extended Kalman Filtering (EKF) technique to predict future harvesting power. The next step is for every energy-aware cycle to generate a calculated model that calculates the energy requirements of diverse security measures and chooses the maximum level of support that meets service needs without using too much power.

Ghimire et al. [12] applied this to IoT network systems, which may detect security threats, put safeguards in place, and prevent assaults from spreading. Several participants may achieve a CS objective by constructing a federation of the shared and learned models. This study's first portion explores the history as well as Federated Learning (FL) comparison, distributed on-site learning, and with centralised learning. An introduction to FL's use in IoT CS follows. In addition to focusing on security, this study includes a diversity of approaches to fixing FL's performance issues, including accuracy, latency, resource limits, and others that might impact the overall security and the performance of the IoT.

Sarker et al. [13] detailed smart cities in education. There is a vast array of possible use cases for existing and future IoT technologies that might automate, increase productivity, and

make consumers' lives easier. Concerning the IoT, smart applications are particularly vulnerable to cyberattacks and other threats. Traditional approaches to protect the IoT are insufficient in light of the present security challenges and the increased proliferation of several forms of attacks and threats. Knowledge of AI, particularly ML and DL solutions, is crucial for developing a cutting-edge security framework to protect the next generation of IoT systems.

Mansour et al. [14] recycled a sickness detection model that combines AI and IoT merging for smart healthcare systems. A disease diagnosis model for diabetes and heart disease may be developed employing AI and IoT combination methodologies; this is the primary goal of this study. Numerous processes, including preprocessing, categorization, data collection, and parameter tweaking, make up the presented model. IoT devices, including sensors and wearables, facilitate data collection, which AI algorithms use to detect illnesses. The proposed method employs the Crowd Search Optimisation-based Cascaded Long Short-Term Memory (CSO-CLSTM) model for illness studies. When it comes to medical data classification, CSO is recycled to fine-tune the "weights" along with "bias" parameters of the CLSTM model.

Hansen et al. [15] discuss how IoT and AI are two of the hottest topics in Industry 4.0. There is a lot of literature on the topics, although much of it is about bigger companies. However, it is of utmost importance that smaller firms have easy access to and can use these technologies since Small and Medium-sized Enterprises (SMEs) are seen as the foundation of various countries' economies. Providing a complete review and study of the adoption of AI and IoT among developed SMEs, this report examines the present hurdles to permitting predictive analytics. It explores the potential benefits of these technologies.

Liang et al. [16] detail how malicious actors may make use of these technologies via cyberthreats, attacks, intrusions, and obfuscation possibilities, all of which are currently being investigated, used, and resolved. Analyse the benefits, drawbacks, and nasty side effects of using ML in CS and IoT/CPS applications in this research. It delves deeply into the many practical applications of ML to security as well as CPS/IoT, especially in improving Intrusion Detection systems (IDs) along with decision accuracy.

More importantly, from a CPS/IoT and security perspective, investigate the risks linked to the incorrect use of machine learning. Throughout the whole technology's lifecycle, with data collection, pre-processing, training, validation, and deployment, there are several methods by which ML systems might be deceived, manipulated, and hacked. Though several approaches have been proposed previously for cybersecurity prevention, some issues remain. The issues occur mostly with the accurate cybersecurity prevention and efficient selection of features. Hence, this work proposes a method considering these limitations with the existing work.

3. Proposed Methodology

As seen in Figure 1, an IoT gateway on the Azure host enables the linking and control of a multitude of IoT devices. The server station receives the NSL-KDD data and uses it to identify the kind of attack. The data is collected in a certain manner that people may benefit from in the event that attacks are not discovered. Creating a blueprint for an IoT smart house is one of the primary goals of this study. IoT vulnerabilities leave smart home design open to assaults, including DoS, data-type probing, along U2R attacks. Identifying and analysing potential security concerns is essential for accurately demonstrating the protection rank of an IoT-based smart home system. In this case, this research provides an optimisation-based solution to identify and safeguard the system in an abnormal condition. This issue has been addressed using three optimisation methodologies.

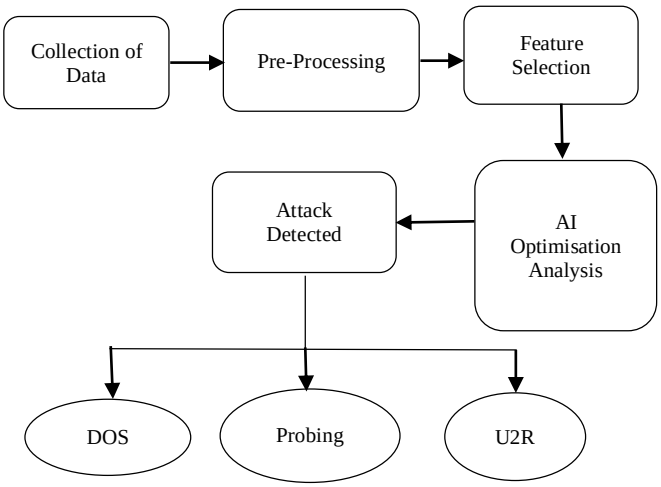

Fig. 1 IoT CS system block diagram for an optimised hybrid AI-based smart house

3.1. Preprocessing

The input data is collected from a dataset. The experimental analysis begins with these two datasets as input data sources [18]. The next step is to get the input data ready to remove noise and missing values. Because of the severe features, the classifiers generated a large number of false alarms. Consequently, preprocessing is crucial. It is impossible to avoid categorization operations due to the fact that certain common traits increase memory and calculating demands. Rough variables are categorised in the following ways in the NSL-KDD dataset:

$$r_s = \{f_{s1} + f_{s2} + \cdots + f_{sn}\} \quad (1)$$

Where n stands for the unique features of the dataset. Rough features are not normal due to the added price and redundancy. These are the altered rough qualities [4].

$$r_s = \{f_{s1}, f_{s2}, f_{s3} \ldots . + f_{sp}\} \quad (2)$$

Where p stands for the most advantageous attributes. Some undesirable characteristics remain even after eradication. Preprocessing is used after the dataset has been analysed to determine its relative importance to maximise the use of the feature collection. To achieve this goal, the research used a range of data preparation approaches, such as cleaning and normalizing [17].

3.1.1. Data Cleaning and Normalization

The data cleaning process removes or corrects errors in data, such as duplication, inaccuracy, irrelevant information, missing data, or improper framing. Since it would be more difficult to draw conclusions if data were necessary for data analysis, data is not needed. Data cleansing also involves purging information [19, 20]. Data cleaning includes erasing unneeded information, fixing modification mistakes, and removing data altogether.

This research aimed to standardise the data analysis and make it easier to discover the necessary data for the research by excluding the data from the data sets. In order to increase the quality by deleting faulty information, it was required to update the missing data because there was already some incomplete or unclear data. Using the MinMax normalisation approach is essential when integrating and normalising data. The feature's minimum value is adjusted to 0, and its maximum value is transformed to 1. The binary representations of all 0s and 1s are transformed. A description of the normalisation technique is given in Equation 3.

$$R_{norm} = \frac{R_i - R_{min}}{R_{max} - R_{min}} \quad (3)$$

In this context, R_i stands for data points, $R_{min}$is the lowest data point value, and R_{max} is the highest data point value. When structured data is present, all three variables work together to establish the normalised value at two specified points in time [17, 18].

Contaminated traffic data will ensure that the data remains suspicious even after complete normalisation for unstructured information. Gathering these characteristics from a wide variety of complicated systems allows us to study attack prediction [23]. The preprocessing output is transferred into FS.

3.2. Feature Selection by PSO

The feature selection gets input from pre-processing. Here, the research provides the FS approach by means of an equation. A 6-tuplet represents FS.

FS=$\{S, A, T, D, f_s, V\}$ Where S is a dataset, S=$\{a_1, a_2, \ldots, a_k\}$ with k instances, A is the features set, A=$\{e_1, e_2, \ldots, e_f\}$ with f count of features, T is a target class, T= $\{c_1, c_2, \ldots, c_n\}$ with n target class classification, D (search space) is a distribution of set A that comprises every subdivision that can be constructed by A, D=$\{s_1, s_2, \ldots, s_l\}$ $(l = 2^n - 1)$ with $s_i = \{e_p, e_q, \ldots, e_r\}$ $(l \leq p \neq q \neq r \leq n)$,V is an evaluation measure also function f_s signifies the transformation of FS: f_s: A → D.Filtering out superfluous characteristics and extracting the optimal subset (s) from a dataset is what FS is all about [21]. The goal of this method is to improve prediction accuracy while decreasing computing complexity and increasing efficiency by selecting a subset of characteristics. Figure 2 and this article both detail the procedures used in FS.

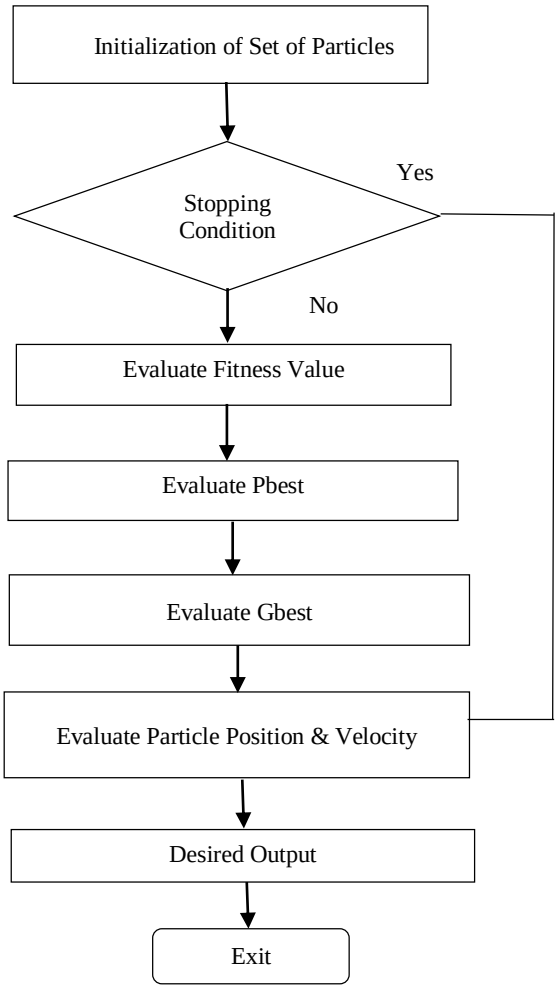

Fig. 2 PSO algorithm flow diagram

1. The generating module prompts the subsequent successor from the first set of features.
2. The estimate module's use of various measurement parameters determines the subsets' applicability.
3. The point at which the subgroup characteristics are considered superior.
4. The program that verifies the features' subsets [24]. The feature selection sends the input to AI optimization for analysis.

3.3. Analysis Using AI

The data analysis is done using FS input data. Prokhorenkova et al. (2018) and Dorogush et al. (2018) proposed a novel gradient-boosting algorithm called CatBoost that uses categorical characteristics with the least amount of information loss. There are various gradient boosting techniques, but CatBoost is unique. To address the issue of target leakage, it first employs boosting, an effective variant of gradient boosting algorithms (Dorogush et al., 2018).

Furthermore, this algorithm performs well on relatively tiny datasets. The third feature that CatBoost is capable of handling is categorization. This processing is often finished during the preprocessing step and basically involves assigning numerical values to the original categorical variables. In addition, CatBoost has been shown to be effective with various data types and formats (Bakhareva et al., 2019). In current centuries, CatBoost has established use in a number of domains, including financial analysis (Xia et al., 2020) and diverse data sources, together with time series data (Diao et al., 2019; Fan et al., 2020).

In particular, instead of using the original variable, this research adds an original binary feature to each category. Dor Ogush et al. (2018) pointed out that the algorithm has the added benefit of avoiding the overfitting that happens with typical gradient-boosting algorithms by using random changes to estimate leaf values while determining the tree structure. The foundational predictor in CatBoost is a binary decision tree. Dorogush et al. (2018) provided the following description of the expected output:

$$Z = H(x_i) = \sum_{j=1}^{J} c_j 1_{\{x \in R_j\}} \quad (4)$$

Where $H(x_i)$ is a decision tree function of the explanatory variables X_i as well as R_j is the disjoint region as per the tree leaves [25]. After AI optimization analysis, the attack is detected.

4. Results

4.1. Dataset

There is no IoT dataset more famous than NSL-KDD. The NSL-KDD dataset is a replica of the original KDD Cup 75 dataset with new, duplicate-free parts. The NSL-KDD dataset comprises 41 features that are classified as either normal links or attack types. The KDD 75 dataset brings to light a number of core issues that were resolved in the NSL-KDD data set [22].

The NSL-KDD training includes a respectable amount of data and test sets. This section provides a detailed description of three NSLKDD attacks: U2R, Sample Attack, and DoS. During the course of a network imaging technique, an attacker may launch a probing attack in an effort to misuse the data acquired. Some examples that gather data from machines linked to the internet include Portsweep, Ipsweep, Satan, Saint, Mscan, and Nmap [18].

4.2. Outcomes

Using the competence achieved for the NSL-KDD data set binary classification, this work evaluates the results of the proposed hybrid optimisation strategy. This research evaluates the precision, recall, accuracy, and F-measure for each attack separately. Computing the TPR allows for the performance measurement to be completed.

One way to put it is as follows: the total number of regular records divided by the number of records mistakenly identified as incursions. The Detection Rate (DR) is the percentage of positive cases accurately recognised compared to the total number of positive instances. There are a few other names for the DR: recall, sensitivity, TPR, and more. The parameters recycled for presentation depth are:

$$\text{True Positive Rate (TPR)} = \frac{TP}{TP+FN} \times 100 \quad (5)$$

$$\text{Precision} = \frac{TP}{TP+FP} \times 100 \quad (6)$$

$$\text{Overall Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \times 100 \quad (7)$$

$$\text{F1-Score} = \frac{2TP}{2TP+FP+FN} \times 100 \quad (8)$$

Table 1. The proposed method is compared to training set ML classifiers

Methods	TPR	Precision	F1 Score	Accuracy
CatBoost	90.45	87.83	88.55	90.78
SVM	97.31	96.08	96.69	96.71
KNN	97.04	97.24	97.11	97.18
LR	96.57	95.07	95.82	95.85
Proposed CatBoost with Optimization	99.45	99.54	99.43	99.76

Various approaches' performance parameters are compared in Table 1. Compared to other models like SVM, KNN, and LR, the proposed model performs better across all parameters. The proposed method is compared to training set ML classifiers. On the NSL-KDD data, the proposed CatBoost method has a TPR of about 99.45%. With a performance gap of 9%, this model beats CatBoost with 2.14% SVM, 2.41% KNN, and 2.88% LR.

Alternatively, the proposed catboost method has a precision of about 99.54%. With a performance gap of 11.71%, this model beats CatBoost by 3.46% SVM, 2.3% KNN and 4.47% LR, while simultaneously, the proposed

CatBoost method has an f1 score of about 99.43%, with a performance gap of 10.99% Catboost, 2.85% SVM, 2.43% KNN, and 3.72% LR. And finally, the proposed CatBoost method has an accuracy of about 99.76%, with a performance gap of 9.89% CatBoost, 3.15% SVM, 2.65% KNN, and 4.07% LR.

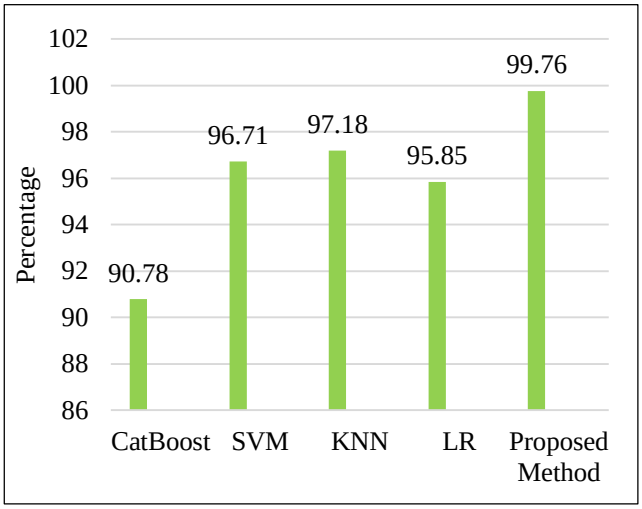

Fig. 3 Comparison of the accuracy of ML classifiers in the training set

Figure 3 shows the proposed strategy is compared to the accuracy of ML classifiers in the training set. This research has planned numerous performance measures, together with the precision, recall, f1 score as well as the accuracy of the system, based on the results, which are enlisted employing the FS technique with the proposed algorithm, which provides the finest accuracy of 99.76% in the training set.

Table 2. The proposed method is compared to testing set ML classifiers

Methods	TPR	Precision	F1 Score	Accuracy
Catboost	89.45	78.63	85.34	86.33
SVM	87.47	77.80	82.35	85.51
KNN	81.07	77.59	83.48	86.66
LR	83.07	79.95	81.48	84.22
Proposed CatBoost with Optimization	90.12	85.11	87.43	90.83

Table 2 shows the proposed method is compared to testing set ML classifiers. Using NSL-KDD data, the proposed CatBoost method has a TPR of about 90.12%. With a performance gap of 0.67%, this model beats CatBoost, 2.65 % SVM, 9.05% KNN, and 7.05% LR.

Alternatively, the proposed CatBoost method has a precision of about 85.11%. With a performance gap of 6.48%, this model beats CatBoost with 7.31% SVM, 7.52% KNN, and 5.16% LR, while simultaneously, the proposed CatBoost method has an f1 score of about 87.43%, with a performance gap of 2.09% for CatBoost, 5.08% SVM, 3.95% for KNN, and 5.95% for LR. And finally, the proposed CatBoost method has an accuracy of about 90.83%, with a performance gap of 4.5% Catboost, 5.32% SVM, 4.17% KNN, and 6.61% LR.

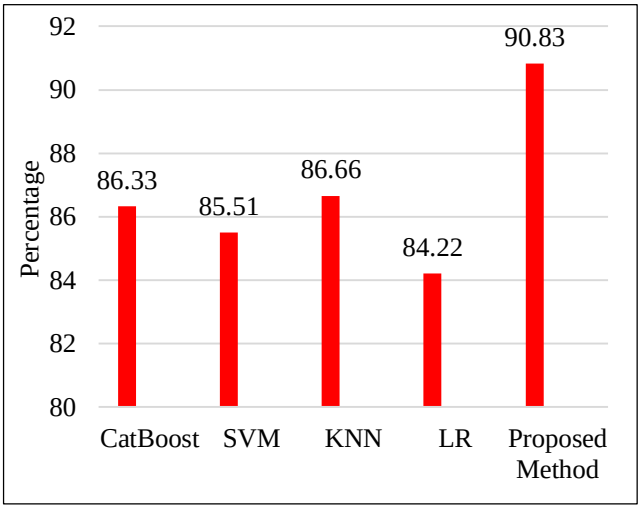

Fig. 4 Comparison of the accuracy of ML classifiers in the testing set

Figure 4 shows the proposed strategy is compared to the accuracy of ML classifiers. The proposed algorithm, which gives 90.83% in the testing set, is measured to have optimized accuracy compared to extra ML classifiers comprising SVM, KNN, LR, and CatBoost algorithms. Superior to more conventional forms of ML, this work discovered that CatBoost with optimisation is the most accurate model.

Table 3. Comparison with [24]

Methods	TPR	Precision	F1 Score	Accuracy
Training Set				
Proposed	99.45	99.54	99.43	99.76
PSO [24]	99.26	99.37	99.31	99.32
Testing Set				
Proposed	90.12	85.11	87.43	90.83
PSO [24]	89.12	81.11	84.92	87.83

From Table 3, it is evident that the proposed method gave improved results when compared to the technique in [24]. Since only optimization is used in [24], and no ML algorithms are used, optimisation using CatBoost and PSO is given in this work. Due to its simplicity, ease of implementation, and bio-inspired search technique (PSO), which uses a single operator to update solutions, this approach outperforms ML classifiers. Efficient solutions may be found for accurate mathematical models.

5. Conclusion

In order to improve the IDS's accuracy and DR, this article explores the use of the PSO algorithm in conjunction with FS. To try to exclude the unnecessary and noisy qualities that have a detrimental impact on the system's pursuit, this work has only employed 10 features from the NSL-KDD dataset.

The main goal of the FS approach is to simplify the dataset by finding the best subset of features and lowering the dataset's dimensionality. Ten out of forty-one features are chosen using the RF algorithm. In order to get the best possible outcome, the PSO algorithm is used with a certain number of iterations and specific particles based on the 10 characteristics that were chosen. The number of particles remains constant at 2800, and the range of iterations is 20–28. After 28 iterations with 2800 particles, the best results as per accuracy along with DR are shown.

The outcomes are contrasted with those of the SVM, LR, and k-NN algorithms used in the dataset's training and testing sets. There is a significant improvement over existing algorithms as per accuracy along with further performance metrics. The findings demonstrate that our approach achieves the greatest accuracy with just 10 features when compared to other algorithms that use the FS technique on the same dataset. The next phase will be finding real-world uses for this research.

References

[1] Hui Wu et al., "Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey," *IEEE Access*, vol. 8, pp. 153826-153848, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Murat Kuzlu, Corinne Fair, and Ozgur Guler, "Role of Artificial Intelligence in the Internet of Things (IoT) Cybersecurity," *Discover Internet of Things*, vol. 1, pp. 1-14, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Diptiben Ghelani, "Deep Learning and Artificial Intelligence Framework to Improve the Cyber Security," *Authorea Preprints*, pp. 1-11, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Aimin Yang et al., "Design of Intrusion Detection System for Internet of Things Based on Improved BP Neural Network," *IEEE Access*, vol. 7, pp. 106043-106052, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[5] Bin Cao et al., "A Many-Objective Optimization Model of Industrial Internet of Things Based on Private Blockchain," *IEEE Network*, vol. 34, no. 5, pp. 78-83, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] Ricardo Jorge Raimundo, and Albérico Travassos Rosário, "Cybersecurity in the Internet of Things in Industrial Management," *Applied Sciences*, vol. 12, no. 3, pp. 1-19, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Mohamed Amine Ferrag et al., "Federated Deep Learning for Cyber Security in the Internet of Things: Concepts, Applications, and Experimental Analysis," *IEEE Access*, vol. 9, pp. 138509-138542, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Hao Xu et al., "A Data-Driven Approach for Intrusion and Anomaly Detection Using Automated Machine Learning for the Internet of Things," *Soft Computing*, vol. 27, pp. 14469-14481, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Claudio Tomazzoli, Simone Scannapieco, and Matteo Cristani, "Internet of Things and Artificial Intelligence Enable Energy Efficiency," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 5, pp. 4933-4954, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] Joey Li et al., "Methods and Applications for Artificial Intelligence, Big Data, Internet of Things, and Blockchain in Smart Energy Management," *Energy and AI*, vol. 11, pp. 1-18, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Bomin Mao, Yuichi Kawamoto, and Nei Kato, "AI-Based Joint Optimization of QoS and Security for 6G Energy Harvesting Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7032-7042, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Bimal Ghimire, and Danda B. Rawat, "Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8229-8249, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Iqbal H. Sarker et al., "Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions," *Mobile Networks and Applications*, vol. 28, pp. 296-312, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Romany Fouad Mansour et al., "Artificial Intelligence and Internet of Things Enabled Disease Diagnosis Model for Smart Healthcare Systems," *IEEE Access*, vol. 9, pp. 45137-45146, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] Emil Blixt Hansen, and Simon Bøgh, "Artificial Intelligence and Internet of Things in Small and Medium-Sized Enterprises: A Survey," *Journal of Manufacturing Systems*, vol. 58, pp. 362-372, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] Fan Liang et al., "Machine Learning for Security and the Internet of Things: The Good, The Bad, and The Ugly," *IEEE Access*, vol. 7, pp. 158126-158147, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[17] Jesús Galeano-Brajones et al., "Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful SDN: An Experimental Approach," *Sensors*, vol. 20, no. 3, pp. 1-18, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[18] By Wang Qi, "Analysis on the Application of Artificial Intelligence in Classroom," *Journal of Physics: Conference Series*, vol. 1345, no. 4, pp. 402-420, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[19] Hongrui Bao et al., "Research on Information Security Situation Awareness System Based on Big Data and Artificial Intelligence Technology," *2019 International Conference on Robots & Intelligent System (ICRIS)*, Haikou, China, pp. 318-322, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[20] S. Shitharth et al., "An Innovative Perceptual Pigeon Galvanized Optimization (PPGO) Based Likelihood Naïve Bayes (LNB) Classification Approach for Network Intrusion Detection System," *IEEE Access*, vol. 10, pp. 46424-46441, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[21] Pratibha Singh, Ajay Verma, and Narendra S. Chaudhari, "Feature Selection-Based Classifier Combination Approach for Handwritten Devanagari Numeral Recognition," *Sadhana*, vol. 40, no. 6, pp. 1701-1714, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[22] Christopher D. McDermott, John P. Isaacs, and Andrei V. Petrovski, "Evaluating Awareness and Perception of Botnet Activity within Consumer Internet-of Things (IoT) Networks," *Informatics*, vol. 6, no. 8, pp. 1-15, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[23] Hassan A. Alterazi et al., "Prevention of Cyber Security with the Internet of Things Using Particle Swarm Optimization," *Sensors*, vol. 22, no. 16, pp. 1-17, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] Nilesh Kunhare, Ritu Tiwari, and Joydip Dhar, "Particle Swarm Optimization and Feature Selection for Intrusion Detection System," *Sādhanā*, vol. 45, pp. 1-14, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[25] Sami Ben Jabeur et al., "CatBoost Model and Artificial Intelligence Techniques for Corporate Failure Prediction," *Technological Forecasting and Social Change*, vol. 166, 2021. [CrossRef] [Google Scholar] [Publisher Link]