INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

An efficient algorithmic technique for feature selection in IoT based intrusion detection system

Alok Kumar Pani[1]*, Manohar M[1], Rajdeep Kumar[2]

1 Department of Computer Science and Engineering, CHRIST (Deemed to be University), Bangalore, India
2 Employee, Banking Industry

OPEN ACCESS

Received: 13.11.2020
Accepted: 26.12.2020
Published: 13.01.2021

Citation: Pani AK, Manohar M , Kumar R (2021) An efficient algorithmic technique for feature selection in IoT based intrusion detection system. Indian Journal of Science and Technology 14(1): 76-85. https://doi.org/10.17485/IJST/v14i1.2057

* **Corresponding author**.

alok.kumar.pani@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Background/Objectives Internet of Things (IoT) is an emerging technology that involves in monitoring the environment and the IoT networks are most vulnerable to attacks due to various number of devices connected in the network. The Intrusion detection technique has been applied to analyze the anomaly in the network. The Existing models have the limitation of inefficiency in the intrusion detection due to the overfit in the models. **Methods/Statistical analysis**: In this research, the Flower Pollination Algorithm (FPA) has been applied in the intrusion detection method to increase the efficiency of the IoT network. The FPA method has the advantage of long distance pollination and flower consistency to analyze the features effectively. The FPA selects the features in the IoT network and apply the features for the classifier to detect the attacks. The classifiers such as Logistic Regression (LR), Support Vector Machine (SVM), Decision Tree (DT), Random Forest (RF) and Artificial Neural Network (ANN) are used to detect the intrusions in the network. **Findings**: This experimental result shows that the proposed FPA method with ANN has the accuracy of 99.5 % in detection and existing ANN has 99.4 % accuracy in detection. **Novelty/Applications**: The FPA method has the advantages of long distance pollination and flower consistency which helps to analyze the network features effectively.

Keywords: Artificial neural network; flower pollination algorithm; internet of things; intrusion detection; long distance pollination

1 Introduction

The embedded devices are connected to the Internet, where the devices can be remotely accessed and used for monitoring refers to the Internet of Things (IoT) paradigm [(1)]. The era of the internet gives rise to smart devices and automated the task and thousands of users are connected to the internet to get the benefits of the promising IoT solutions [(2)]. These applications include the health care system, home automation, smart grids and smart cities [(3)]. The IoT system involves in low security due to the resource constraint devices and many number of devices connected in the IoT [(4)]. IoT provides the many

solutions as it provides information through the internet and user can access in remote areas. However, the hacker may take advantages of the IoT devices, which is a threatening to privacy and security of the user For example, the Denial-of-Services (DDoS) attacks affects the IoT devices and provide the information to the hackers [5]

An Intrusion Detection System (IDS) is the method that process in the network layer of an IoT system [6]. Machine learning techniques has been applied in the IDS and observed the higher performance in the identifying the intrusion and malware [7,8]. The existing method involves in IDS tends to be ineffective due to drawbacks of big data, centralization and low privacy [9]. The existing method is also inefficient in handling the streaming data of IoT system. Most of the method in the IDS has low efficiency in the intrusion detection to increase the efficiency of the detection [10,11]. In this research, the FPA is proposed in the IoT intrusion detection to increase the efficiency of the detection. The FPA method has the advantages of the long distance pollination and the flower consistency that effectively analyze the feature. The classifiers such as Logistic regression, SVM, ANN, decision tree and RF are used to analyze the performance of the proposed FPA method in IoT intrusion detection.

The organization of the paper is given as follows: Literature survey of the recent techniques in IoT intrusion detection is provided in Section 2. The proposed FPA and the classifier explanation is given in the section 3 and the experimental results are shown in the section 4. The conclusion of the research is provided in the Section 5

2 Literature survey

Internet of Things (IoT) technology has the advantages of more flexibility in monitoring the environment. The IoT has the limitation of low security, due to a number of devices are connected to the IoT network with low resources. Intrusion detection technique has been applied in the IoT system to detect the anomaly behavior in the system. The recent research in the intrusion detection of IoT were surveyed in this section.

Hasan et al. [12] applied the several machine learning algorithms such as Logistic Regression (LR), Support Vector Machine (SVM), Decision Tree (DT) etc.., in the IoT for intrusion detection system. The developed method is evaluated on dataset consists of seven types of attacks and thirteen features for the detection. The experimental result shows that the developed method has high performance on the intrusion detection data. The result shows that the decision tree, random forest and Artificial Neural Network (ANN) has more accuracy and the random forest has more performance on different metrics. The ANN has the accuracy of 99.4 % and random forest has the accuracy of 99.4 % in DS2OS dataset. The random forest and ANN have the limitation of overfitting in the model for a large number of data.

Li et al. [13] developed the framework of Collaborative Blockchained Signature based Intrusion Detection System (CBSigIDS). This method can incrementally create and update a trusted signature database in the collaborative IoT environment. The CBSigIDS verifies the distributed architectures without the need of a trusted node. The experimental result shows that the CBSigIDS increases the effectiveness of the Intrusion detection system in the critical scenarios. The accuracy of the classification was achieved as 66.7 % in attack detection in the network. The classification performance of CBSigIDS is low and machine learning technique was required to improve the classification performance.

Pan et al. [14] presented the context-aware intrusion detection for the Building automation system. The streaming heterogeneous information were used to develop the runtime mode for the functionality patterns and service interactions. The developed intrusion detection system analysis shows the anomaly behavior in the network to detect the intrusion. The context-aware intrusion detection system is evaluated by generating several attacks in the BACnet protocol and the result shows that the developed method has the high performance in detecting the attacks. The developed system has FPR of 0.35 for attack classification in the intrusion detection method. The system has lower efficiency in classification due to model's inability to handle complex and large dataset.

Yahalom et al. [15] proposed the method for automatically learning the hierarchy subclass in the normal instance of dataset to reduce the False Positive Rate (FPR) compared to the existing method in the intrusion detection. This method requires user data to analyze the hierarchy or make assumptions about its distribution. The developed method was evaluated on the operational networks of IP cameras and IoT devices which attacks on communication protocol. The experimental result shows that the performance of the developed method is high in the detection. The system has the True Positive Rate (TPR) of 0.752 and False Positive Rate (FPR) of 0.039 values. The hierarchy size of the method was more and it required to reduce the hierarchy size to apply in IoT devices. This method needs to be analyzed in the common message transmission protocol of MQTT.

Diro et al. [16] analyze the automatic learning performance of the deep learning techniques in the pattern discovery and applied in the intrusion detection system. The deep learning technique is applied in the intrusion detection in IoT network and the deep learning performance in the intrusion detection is high compared with the traditional machine learning algorithm. The deep learning was evaluated against the distributed attacks. The experiment result shows that the deep learning method has the higher performance in the detection system. The deep learning method has F1-measure of 99.24 % in the attack detection and limitation of overfitting problem that affects the accuracy of the classification.

Liang et al.[17] proposed a hybrid strategy of multi-agent system, block chain and deep learning method for the intrusion detection in IoT system. The NSL-KDD dataset was used to evaluate the performance of the hybrid strategy method. This analysis shows that the deep learning method has higher efficiency in detecting attacks from transportation layer. The accuracy of the hybrid strategy method was achieved as 91.5 % in the intrusion detection system. The overfitting problem in the deep learning method needs to be solved to improve the efficiency of detection system.

The existing method has the drawback of the lower performance in the detection of the intrusion on IoT. To overcome the limitation of the existing method, the FPA method is proposed to increase the performance of the Intrusion detection in IoT.

3 Proposed Method

The security in IoT is vulnerable due to the various number of nodes connected in the IoT network and the IoT devices are low constrain devices. This research aims to increase the efficiency of the machine learning technique in the intrusion detection with the FPA feature selection method. The machine learning techniques such as logistic regression, SVM, RF etc.., is applied to analyze the performance of the proposed FPA method. The FPA has the advantages of long-distance pollination and flower consistency that helps in analyzing the feature effectively. The preprocessing technique is applied to eliminate the missing data and the input data is converted into the vector to process the machine learning. The dataset of the intrusion detection is used to analyze the performance of the method. The architecture of the proposed FPA method in the IoT intrusion detection is shown in the Figure 1.

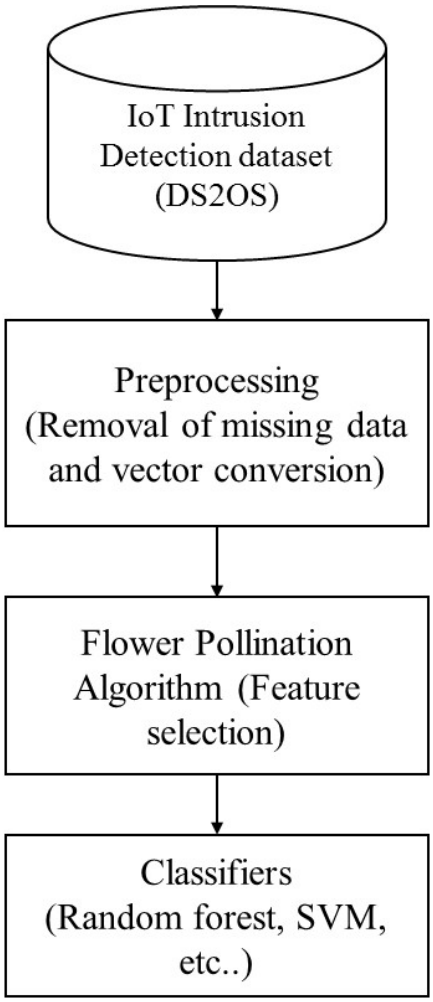

Fig 1. The architecture of the proposed FPA method in IoT intrusion detection

3.1 Dataset

The dataset of DS2OS is collected from kaggle[18]. The research[19] creates the virtual IoT environment based on Distributed Smart Space Orchestration System (DS2OS) to create synthetic data. The architecture is a collection of micro-services that communicate based on the Message Queuing Telemetry Transport (MQTT) protocol. The dataset consists of 357,952 samples and 13 features with normal data of 347,935 and anomalous data of 10,017 that contains eight classes, which is used for classification. Features "Accessed Node Type" and "Value" contain the missing data of 148 and 2050, respectively.

3.2 Preprocessing

The "Accessed Node Type" column and "Value" column in DS2OS dataset contain missing data that rise the anomaly in data transferring. "Accessed Node Type" feature has categorical value and the "Value" feature has continuous values. Apart from this, the timestamp column is eliminated from the dataset as this has a minimum correlation in the dataset's predicator variable normality.

The categorical data in the dataset are classified as ordinary and nominal values, and the numerical dataset is classified into Discrete and Continuous values. The next process involves in categorize the data into vectors and there are many ways to convert the values into vectors. The Label encoding and one hot encoding are commonly used technique. In this research, label encoding techniques are used to convert the data into a feature vector. Most of the dataset features contain nominal categorical value and many unique values. The label encoding technique is applied in the dataset to convert values into a vector.

3.3 Flower pollination algorithm

The FPA method is the recent optimization technique and it has been used in the global optimization process that provides the robust performance. The FPA technique used in this research for feature selection in the IDS in IoT system. The FPA method is proposed in the research[20,21], to idealize the flower pollination process with flower constancy and pollinator behavior. The four major rules involve in the FPA is given as follows:

1. In the global pollination process, the biotic and cross-pollination is considered and performed based on the L'evy flights technique.
2. In local pollination process, abiotic and self-pollination is performed.
3. Flower constancy is considered as the reproduction probability that is proportional to the two similar flowers involved
4. A switch probability $p \in [0,1]$ is applied to control the global and local pollination. The physical proximity and other factors such as wind local pollination have the influence on the fraction p in the overall pollination activities.

The flower constancy is represented in the Eq. (1)

$$x_i^{t+1} = x_i^t + \in \left(x_j^t - x_k^t\right) \tag{1}$$

Where x_t^j and x_t^k are denoted as pollen from the different flowers of the same plant species. This mimic the flower constancy in the limited neighborhood. Mathematically, if x_t^j and x_t^k are comes from same species or selected from same population and if draw ⊠ from a uniform distribution in [0, 1], then it denotes the local random walk.

An initial value is denoted as $p = 0.5$ and the parametric study is applied to identify the most appropriate parameter range. In the simulation, the $p = 0.8$ is set in process for the most applications.

3.4 Logistic regression

The Logistic Regression is discriminative model that performs depend on the dataset quality. Assume the features $X = X_1, X_2, X_3, \ldots X_n$ (where, $X_1 - X_n =$ Distinct features) , with weights $W = W_1, W_2, W_3 \ldots W_n$ bias $b = b_1, b_2, \ldots b_n$ and classes $C = c_1, c_2, ..c_n$ from the dataset. The equation of posterior is provided in the Eq. (2).

$$\text{Predicted value} : p(y = C \mid X; W, b) = \frac{1}{(1 + \exp(-W^T X - b))} \tag{2}$$

3.5 Support vector machine

Support Vector Machine (SVM) is a supervised learning model for the data analyzing and used for the classification, regression and outlier's detection [12] and SVM is mostly applied in the Non-linear data. The hyperplane is developed based on the closest points in high dimensional space. SVM process the sum of distances between hyper plane points to closes points in high dimensional space to measure margin. The margin boundary function is given in Eq. (3).

$$\text{Minimise } W(\alpha) = \frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N} y_i y_j \alpha_i \alpha_j k(x_i, x_j) - \sum_{i=1}^{N} \alpha_i \tag{3}$$

Where, $\forall_i : 0 \leq \alpha_i \leq C$ and $\sum_{i=1}^{N} \alpha_i y_i = 0$

The Radial Basis Function is used in this research to calculate hyper plane margin, as shown in Eq. (4).

$$k(x_i, x_j) = \exp\left(-\gamma \left\| x_i - x_j \right\|^2\right), \gamma > 0 \tag{4}$$

3.6 Decision tree

The Decision Tree (DT) method allows each node to weight possible action against one another based on the benefits, cost and probabilities. The possible outcomes of a series of related choices are mapped [12] and a DT starts from the single node and branches into possible outcomes. Each outcomes leads to additional nodes that branch off into other instances and this is tree-like shape and in the other form, a flowchart-like structure. Consider a binary tree, where a parent node is split into two nodes such as a left child and a right child. The parent node, left child and right child have the data of P_d, LC_d, RC_d , respectively [12]. Assume feature x, impurity measure is denoted as I (data), the number of samples in parent node is denoted as P_n , the number of left child is denoted as LC_n and the number of samples in right child is denoted as RC_n; DT's target is to maximize the following Information Gain in Eq. (5).

$$\text{Information Gain}(P_d, x) = I(P_d) - \frac{LC_n}{p_n} - \frac{RC_n}{P_n} I(RC_d) \tag{5}$$

3.7 Random forest

The Random Forest (RT) is supervised the classification algorithm which creates the forest with many decision trees based on the features form of dataset and the RF method has the advantages of high execution speed [12]. Many decision trees are combined to form a random forest and this is predicted based on the average predictions of each component tree. This method usually has the better predictive accuracy than a single decision tree and more trees in the forest increase the performance of the method.

One tree process is described by considering $P_i \in \square^{M_i \times N_i}$ where the i^{th} partition of samples (M_i) is defined as $i$and features (N_i) . The P_i are selected to generate random samples from the original data $\left(X \in \square^{M \times N}\right)$ and the available samples $(M_i)$are split based on a subset feature N_i at each node. The Gini index is used to measure the best splitting feature and cut-off points. The samples having values is high compared to cut-off values are directed to the right node (v_R), otherwise this is sent to left node (v_L). The samples are moved from the root node (v_n) to terminal nodes after several splits are performed. The samples moved to the terminal nodes are considered as terminal leaves that supply the samples prediction. Ensemble prediction of forest $Y \in \square^{M \times 1}$ is measured from individual trees combination.

Classification: $Y_i = \text{ mode }_{-}(n = 1 \ldots N_{\text{trees}} Y_n)$

3.8 Artificial neural network

Artificial Neural Network (ANN) is the machine learning technique that is the basic for various deep learning algorithms. The raw data are used to train the ANN and this method has more number of turning parameter that makes the complex structure [22]. This method requires more computation time to optimize the error than other techniques. For this purpose, the Neural Network algorithm are trained in the Graphics Processing Unit (GPU) using CUDA programming. Each node of ANN is trained with the feature set $X = X_1, X_2, X_3, ..X_n$. The features are multiplied using some random weights, $W = W_1, W_2, W_3 \ldots W_n$ and added with bias values, $b = b_1, b_2, \ldots b_n$. The values are provided as input to the non-linear activation function [12]. The Activation function can be of several types, Following Eq. (6) represent some activation function.

$$L\left(\hat{y}^i, y^i\right) = -\left(y^i \log\left(\hat{y}^i\right) + \left(1 - y^i\right) \log\left(1 - \hat{y}^i\right)\right) \tag{6}$$

The performance of the classifier and the classifier with the proposed FPA method is tested in the dataset. The experimental result of the proposed FSA method in the IoT intrusion detection is shown in the following section.

4 Experimental result

Many embedded devices are connected to the Internet and used it for the monitoring purpose, hence its termed as "IoT". IoT system are vulnerable due to the various number of devices are connected to the network and attacking one device can access the data on the network. Intrusion detection technique has been applied to the IoT system to find the attacks and abnormality in the network. The FPA method is proposed in the IoT intrusion detection system to increase the efficiency of the detection. The classifiers are analyzed in the intrusion system with and without FPA method. The proposed method is performed on the system consists of intel i5 processor with 8 GB RAM and 500 GB hard disk. The pandas and numpy framework are used in python to execute the proposed method. The scikit-learn framework and keras framework were are used in the method. The various classifiers are used to analyze the performance of the FPA method. The metrics such as accuracy, precision, recall and f-measure are calculated from the proposed FPA method. The formula for measuring the accuracy, precision, recall and f-measure are shown in the Eq. (7-10), respectively.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \tag{7}$$

$$\text{Precision} = \frac{TP}{TP+FP} \tag{8}$$

$$\text{Recall} = \frac{TP}{TP+FN} \tag{9}$$

$$F-\text{measure} = 2\times\frac{\text{Precision}\times\text{Recall}}{\text{Precision}+\text{Recall}} \tag{10}$$

Where, TP denotes the True Positive, FP denotes the False Positive, TN denotes the True Negative, and FN denotes the False Negative. The performance of the proposed method is analysed and compared with existing methods.

4.1 Performance analysis

The proposed FPA method is evaluated in the IoT intrusion detection to analyse its effectiveness. The standard DT, RF and ANN classifiers and the proposed FPA method is compared to analyze the efficiency of the system.

Table 1. The Performance Analysis of the Various Classifier in IoT Intrusion Detection

Methods	LR[12]	FPA-LR	SVM[12]	FPA-SVM	DT[12]	FPA-DT	RF[12]	FPA-RF	ANN[12]	FPA-ANN
Accuracy	98.3	98.7	98.2	98.5	99.4	99.5	99.4	99.5	99.4	99.5
STD(+/-)	0.0055	0.0052	0.0064	0.0058	0.016	0.012	0.014	0.12	0.021	0.14
Precision	98	98.4	98	98.45	99	99.2	99	99.2	99	99.1
Recall	98	98.6	98	98.58	99	99.2	99	99.2	99	99.1
F1-Score	98	98.4	98	98.5	99	99.2	99	99.2	99	99.1

The various classifiers are used to test the performance of the proposed FPA method in IoT intrusion detection. The classifiers such as LR, SVM, DT, RF and ANN were applied with proposed FPA to test the performance, as shown in Table 1. The existing ANN method[11] doesn't select the relevant features and proposed FPA-ANN method selects the relevant features to improve the efficiency of the classification. The result shows that the proposed FPA method has the higher performance compared to the existing method. The proposed FPA method has the higher accuracy of 99.5 % compared to the standard ANN has the accuracy of 99.4 %. The FPA method has the advantages of the long-distance pollination and flower consistency, which increase the performance of the feature analysis. The long-distance pollination helps to analyze more feature and flower consistency helps to select more relevant features.

The accuracy of the various methods with FPA feature selection in the IoT intrusion detection is compared in the Figure 2. The classifier with FPA feature selection method is achieved accuracy compared to the existing classifiers. The proposed FPA-ANN method selects the relevant features for the classification that improves the efficiency of the classification and existing ANN method [12] selects the features from the dataset without analysis. The FPA method has the advantage of better convergence that improve the efficiency of the intrusion detection model. The FPA with RF classifier has the accuracy of 99.5 %, while the existing RF method has the accuracy of 99.4 % in the IoT intrusion detection. The FPA method with the DT and ANN achieved high accuracy.

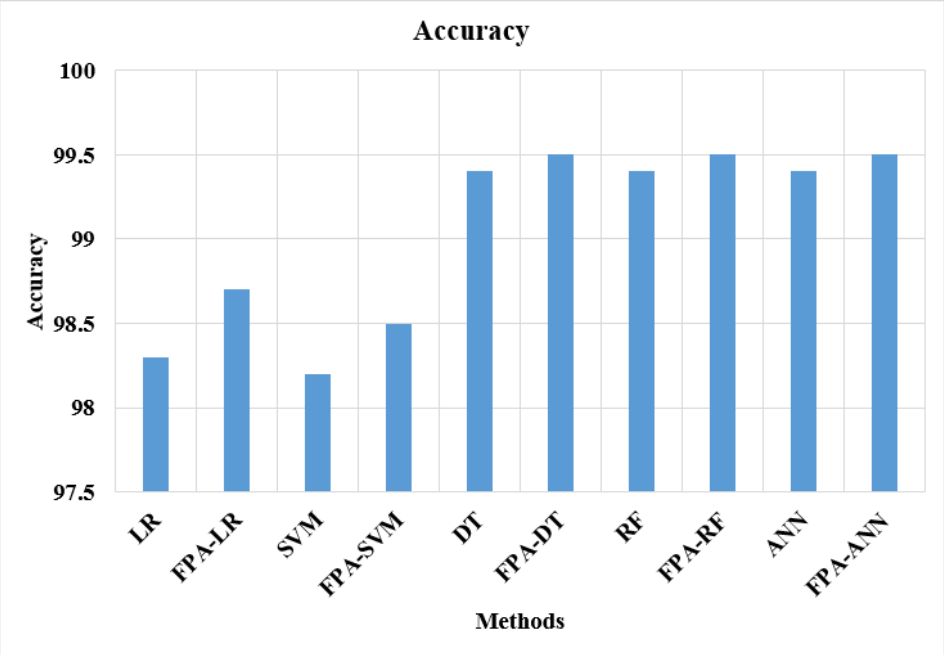

Fig 2. Accuracy of the proposed FPA in IoT intrusion detection

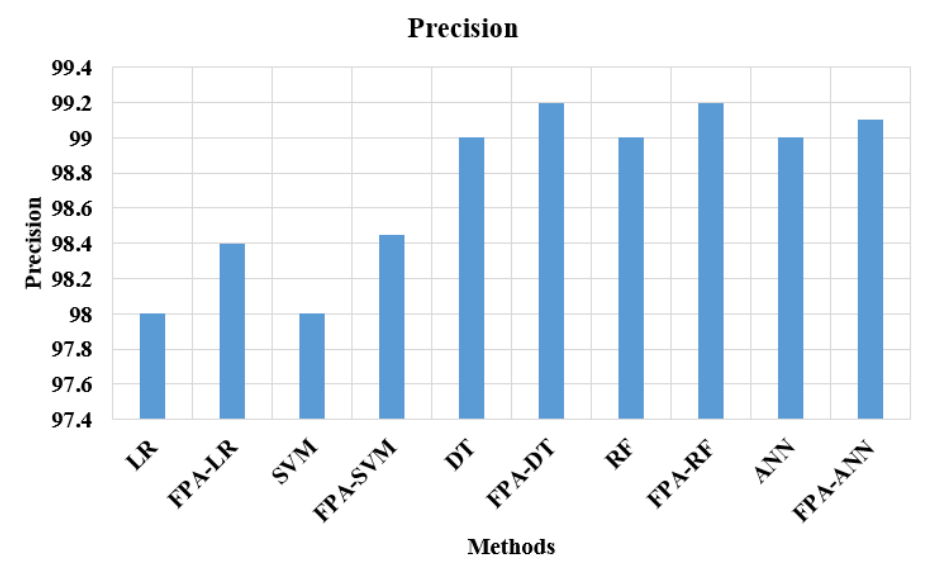

Fig 3. The precision value of the various methods in IoT intrusion detection

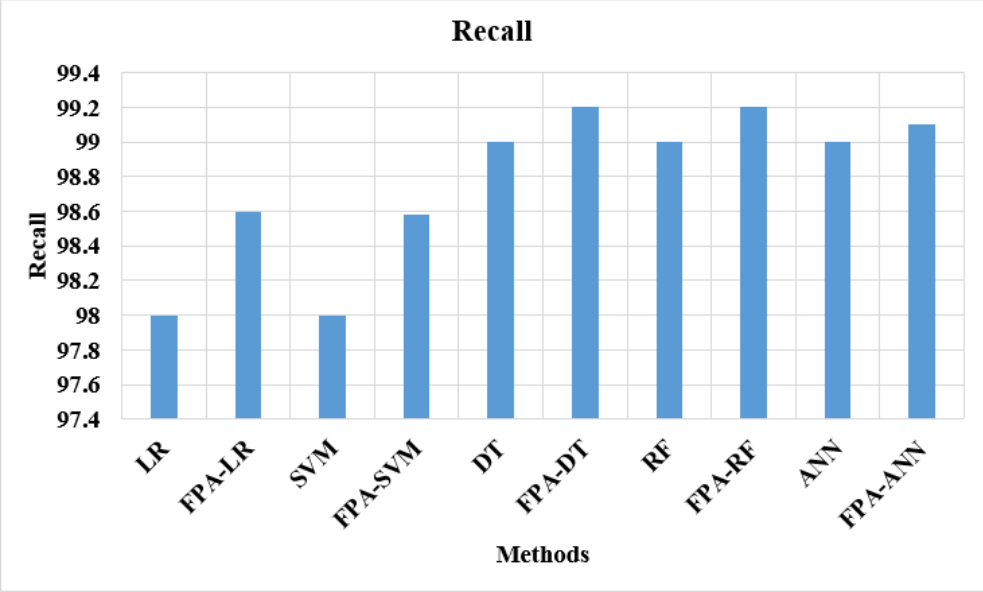

Fig 4. Recall value of the proposed FPA method in IoT intrusion detection

The precision value for the various method in the IoT intrusion detection is measured and shown in the Figure 3. The high precision value is achieved using the FPA in the feature selection method. The FPA method has better convergence that provides the relevant features for the classifier to improve the efficiency of the method. The FPA feature selection method increases the precision value in the IoT intrusion detection system. The FPA-ANN has the precision value of 99.1 % and the standard method has the precision value of 99 %.

The recall value of the proposed FPA method in IoT intrusion detection is compared with the standard classifier as shown in the Figure 4. The classifiers with the FPA feature selection technique achieves the higher recall value than the standard methods. The FPA-ANN has the recall value of 99.1 % compared to the ANN method with 99 %.

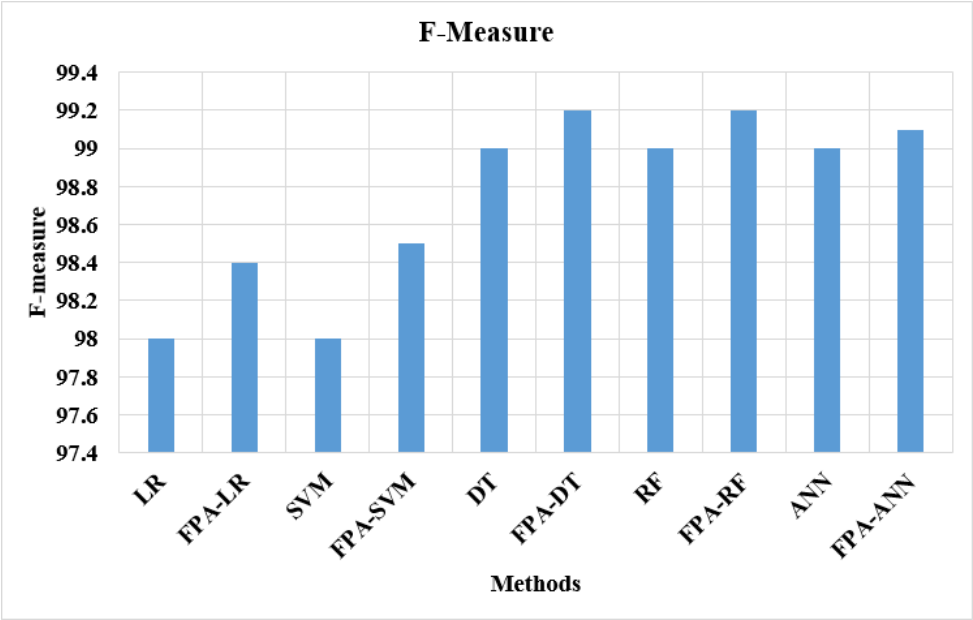

Fig 5. F-measure value of the proposed FPA method in IoT intrusion detection

The F-measure of proposed FPA method is compared with various existing methods in the IoT intrusion detection system, as shown in Figure 5. The FPA method has the better convergence that improves the efficiency of the classification. ANN method has the higher efficiency to handle the non-linear data that improves the performance of the classification. The proposed FPA method has the higher F-measure value compared to the existing classifiers. The FPA method is applied to the feature selection method and the various classifiers are used to detect the intrusion. This shows that the proposed FPA in the IoT intrusion detection has the higher performance compared to the standard existing method.

Therefore, the comparison analysis shows that the proposed FPA method has the higher performance in the IoT intrusion system compared to the standard DT, RF and ANN classifiers.

5 Conclusion

The security in IoT environment is low because of the vast number of devices in the IoT network and the data can be accessed from a single node. The intrusion detection in the IoT network detects the attacks in the network. In this research, the FPA is proposed to select the features in the intrusion detection for feature selection. The FPA method has the advantage of long distance pollination that analyzes number of features and flower consistency, which provides more relevant features for the detection. The performance of the proposed FPA is tested with various classifications in the IoT intrusion detection system. The proposed FPA method has the better convergence process and selects the relevant features for the detection. The ANN has the higher efficiency to handle the non-linear data that improves the detection performance. The proposed FPA with the ANN has the accuracy of 99.5 % compared with the standard ANN which has the accuracy of 99.4 %. In the future work, the proposed method is involved in encrypting the data for the IoT system.

Acknowledgments

We thank CHRIST (Deemed To Be University), Bangalore for providing a favourable environment to carry out our research work.

References

1) Mukherjee A, Deb P, De D, Buyya R. IoT-F2N: An energy-efficient architectural model for IoT using Femtolet-based fog network. *The Journal of Supercomputing*. 2019;75(11):7125–7146. Available from: https://dx.doi.org/10.1007/s11227-019-02928-0.
2) Chowdhury A, Raut S. Scheduling Correlated IoT Application Requests Within IoT Eco-System: An Incremental Cloud Oriented Approach. *Wireless Personal Communications*. 2019;108:1275–1310. Available from: https://dx.doi.org/10.1007/s11277-019-06469-w.
3) Yu J, Bang HC, Lee H, Lee YS. Adaptive Internet of Things and Web of Things convergence platform for Internet of reality services. *The Journal of Supercomputing*. 2016;72(1):84–102. Available from: https://doi.org/10.1007/s11227-015-1489-6.
4) Mukherjee B, Wang S, Lu W, Neupane RL, Dunn D, Ren Y, et al. Flexible IoT security middleware for end-to-end cloud–fog communication. *Future Generation Computer Systems*. 2018;87:688–703. Available from: https://dx.doi.org/10.1016/j.future.2017.12.031.
5) Casola V, Benedictis AD, Riccio A, Rivera D, Mallouli W, de Oca EM. A security monitoring system for internet of things. *Internet of Things*. 2019;7. Available from: https://dx.doi.org/10.1016/j.iot.2019.100080.
6) Elrawy MF, Awad AI, Hamed HFA. Intrusion detection systems for IoT-based smart environments: a survey. *Journal of Cloud Computing*. 2018;7(1). Available from: https://dx.doi.org/10.1186/s13677-018-0123-6.
7) Dovom EM, Azmoodeh A, Dehghantanha A, Newton DE, Parizi RM, Karimipour H. Fuzzy pattern tree for edge malware detection and categorization in IoT. *Journal of Systems Architecture*. 2019;97:1–7. Available from: https://dx.doi.org/10.1016/j.sysarc.2019.01.017.
8) Prabhakaran V, Kulandasamy A. Integration of recurrent convolutional neural network and optimal encryption scheme for intrusion detection with secure data storage in the cloud. *Computational Intelligence*. 2020;2020:1–27. Available from: https://dx.doi.org/10.1111/coin.12408.
9) Rathore S, Kwon BW, Park JH. BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. *Journal of Network and Computer Applications*. 2019;143:167–177. Available from: https://dx.doi.org/10.1016/j.jnca.2019.06.019.
10) Deng L, Li D, Yao X, Cox D, Wang H. Mobile network intrusion detection for IoT system based on transfer learning algorithm. *Cluster Computing*. 2019;22(S4):9889–9904. Available from: https://dx.doi.org/10.1007/s10586-018-1847-2.
11) Stylianopoulos C, Johansson L, Olsson O, Almgren M. CLort: High Throughput and Low Energy Network Intrusion Detection on IoT Devices with Embedded GPUs. *Nordic Conference on Secure IT Systems*. 2018;p. 187–202. Available from: https://doi.org/10.1007/978-3-030-03638-6_12.
12) Hasan M, Islam MM, Zarif MII, Hashem MMA. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet of Things*. 2019;7. Available from: https://dx.doi.org/10.1016/j.iot.2019.100059.
13) Li W, Tug S, Meng W, Wang Y. Designing collaborative blockchained signature-based intrusion detection in IoT environments. *Future Generation Computer Systems*. 2019;96:481–489. Available from: https://dx.doi.org/10.1016/j.future.2019.02.064.
14) Pan Z, Hariri S, Pacheco J. Context aware intrusion detection for building automation systems. *Computers & Security*. 2019;85:181–201. Available from: https://dx.doi.org/10.1016/j.cose.2019.04.011.
15) Yahalom R, Steren A, Nameri Y, Roytman M, Porgador A, Elovici Y. Improving the effectiveness of intrusion detection systems for hierarchical data. *Knowledge-Based Systems*. 2019;168:59–69. Available from: https://dx.doi.org/10.1016/j.knosys.2019.01.002.
16) Diro AA, Chilamkurti N. Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*. 2018;82:761–768. Available from: https://dx.doi.org/10.1016/j.future.2017.08.043.

17) Liang C, Shanmugam B, Azam S, Karim A, Islam A, Zamani M, et al. Intrusion Detection System for the Internet of Things Based on Blockchain and Multi-Agent Systems. *Electronics*. 2020;9(7):1120–1120. Available from: https://dx.doi.org/10.3390/electronics9071120.
18) Pahl MO, Aubet FX. DS2OS traffic traces. 2019. Available from: https://www.kaggle.com/francoisxa/ds2ostraffictraces.
19) Pahl MO, Aubet FX. All eyes on you: Distributed Multi-Dimensional IoT microservice anomaly detection. In: and others, editor. 14th International Conference on Network and Service Management (CNSM). 2018;p. 72–80.
20) Yang XS. Flower pollination algorithm for global optimization. In: and others, editor. International conference on unconventional computing and natural computation. Springer. 2012;p. 240–249. Available from: https://doi.org/10.1016/j.eswa.2016.03.047.
21) Zhang P, Liu F, Aujla GS, Vashisht S. VNE strategy based on chaos hybrid flower pollination algorithm considering multi-criteria decision making. *Neural Computing and Applications*. 2020;4:1–2. Available from: https://dx.doi.org/10.1007/s00521-020-04827-5.
22) Karim A, Azam S, Shanmugam B, Kannoorpatti K, Alazab M. A Comprehensive Survey for Intelligent Spam Email Detection. *IEEE Access*. 2019;7:168261–168295. Available from: https://dx.doi.org/10.1109/access.2019.2954791.