Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 2s (2024)

Enhancing Internet of Things Security Through Optimization Algorithms and Machine Learning

Zakiya Manzoor Khan

Department of Computer Science and Engineering

Lovely Professional University

Phagwara, Jalandhar, Punjab

zakiyamanzoorkhan@gmail.com

Article History:

Received: *14-04-2024*

Revised: *22-05-2024*

Accepted: *06-06-2024*

Abstract:

IoT network traffic classification is an approach used to analyze IoT network traffic, revealing various network activities. The network traffic analysis process involves several steps: data input, preprocessing, feature extraction, classification, and performance analysis. Although various machine learning algorithms have been proposed in recent years, they have failed to achieve high accuracy and effectively extract features from datasets. This research aims to develop an algorithm that can extract features and achieve high accuracy in network traffic classification.To accomplish this, a hybrid optimization algorithm combining genetic algorithms and Particle Swarm Optimization (PSO) is proposed. This hybrid algorithm extracts features, which are then classified using Random Forest. The proposed model is implemented in Python, and its performance is evaluated in terms of accuracy, precision, and recall.

Keywords: IOT, PSO, Genetic, Random Forest.

1. INTRODUCTION

In the contemporary world, an extensive network known as the Internet of Things (IoT) connects billions of devices, facilitating communication between them. Coined by Kevin Ashton in 1999 during his work on supply chain optimization at Proctor & Gamble, the term has evolved over two decades, encompassing diverse applications in fields like healthcare, agriculture, utilities [1], and transportation. Despite this evolution, the fundamental aim of IoT remains consistent: enhancing efficiency and delivering information swiftly without relying solely on human interactions. Over the past five years, IoT has experienced significant growth. Projections suggest that the number of IoT devices will surge to 38.6 billion in 2025 and reach 50 billion by 2030. These devices continually gather various data from users, including browsing history, location, contacts, calendar events, and health records [2]. The primary motivations behind collecting such sensitive data are convenience and the enhancement of efficiency through smart device usage. As devices become more intelligent, they adeptly respond to daily needs, such as automatically adjusting lights at specific times, handling emergencies like fires, or addressing security concerns through advanced security systems. However, the daily convenience offered by these devices also introduces significant security risks.

Smart devices within the Internet of Things (IoT) network store highly personalized and private information [3]. Unauthorized access to such data by individuals or agents can lead to substantial harm to the user's well-being and safety. For instance, hackers could seize control of self-driving vehicles,

potentially causing severe harm to the driver, or infiltrate home security cameras, violating privacy. The diverse range of IoT devices introduces security and privacy challenges. Without a secure system enabling these devices to exchange information privately, new IoT devices may fail to meet user expectations, discouraging users if their personal data cannot be adequately safeguarded. IoT networks present unique challenges, including privacy concerns, authentication issues, storage limitations, and data processing speeds [4]. Additionally, IoT devices themselves often lack essential security modules and software, creating vulnerabilities that cyber attackers can exploit. As IoT devices continue to advance, ongoing research is crucial to explore new techniques that can enhance their security. IoT applications can be categorized into three layers: the application layer, the network layer, and the physical layer [5]. Each layer encompasses various technologies that may be susceptible to security risks such as Distributed Denial of Service (DDOS) attacks. The physical layer, also known as the perception layer, encompasses various data sensors such as RFID, gateways, and barcodes. Its primary function is to collect data from the device's surroundings and transmit it to the network layer for further processing. The network layer's objective is to relay the data collected by the physical layer to a data processing source through a network [6]. Lastly, the application layer serves as an interface between end users and the network layer, facilitating user interaction. Security in IoT devices poses a significant challenge in today's landscape, given the heterogeneity and extensive interconnectivity of devices. Potential attackers can compromise IoT systems by exploiting physical vulnerabilities, manipulating network or routing protocols, or employing encryption attacks to gain unauthorized access to devices [7]. These vulnerabilities lead to the classification of IoT attacks into three main categories: attacks on the physical layer, attacks on the network layer, and attacks on the application layer. Physical layer attacks focus on hardware devices, network layer attacks target the IoT system's network, and application layer attacks employ malware, trojans, and viruses to compromise the application layer. Figure 1 illustrates a layer-wise breakdown of attacks in IoT systems [8].

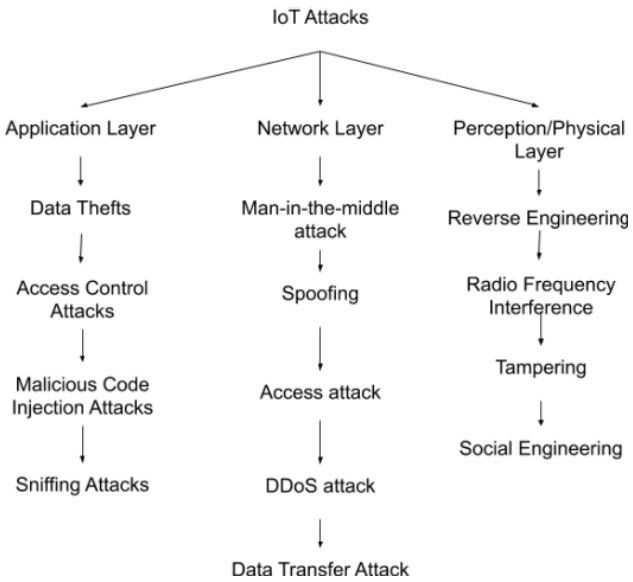


Fig 1: IoT security attacks by layer

1.1 Physical Layer Attacks.

Physical attacks serve as a means to uncover new vulnerabilities within IoT systems, primarily targeting the hardware devices. These attacks encompass various techniques, including but not limited to reverse engineering, radio frequency interference, tampering, and social engineering [9].

- *Reverse Engineering:* In reverse engineering, an attacker systematically disassembles a device to identify vulnerabilities. By compiling a list of both known and unknown vulnerabilities, the attacker can exploit these issues on other devices within a related network.
- *Radio Frequency Interference:* This involves an attacker using a device to disrupt the connectivity of IoT devices through radio frequency interference. Jamming and RF interference occur when the attacker is in close proximity to the device's location [10].
- *Tampering:* Tampering occurs when an attacker physically alters an IoT device. Through tampering, the attacker gains access to sensitive information such as login credentials and encryption keys.
- *Social Engineering:* Social engineering entails the manipulation of end users to get confidential data.

1.2 Network Layer Attacks.

At the network layer, IoT devices utilize the network to transmit information received from the physical layer to a server or device for processing. The following are some attacks and security threats identified at the network layer [11]:

- *Man in the Middle Attack*
  A man-in-the-middle attack captures and alters data between two nodes in the IoT network. Data packets not directly communicating between devices can be intercepted by all nodes in the network, allowing devices to intercept and read the contents. The objective of this attack is to modify data on the IoT network and disrupt traffic. Given the prevalence of open and unsecured devices in IoT networks, these devices can serve as potential entry points for a man-in-the-middle attack.
- *Spoofing*
  Data in IoT networks are encrypted and transmitted through network traffic via routing protocols using IP addresses. An attacker can replicate, alter, or resend IP addresses through transport protocols, causing disruptions in network traffic [12]. To execute spoofing attacks in IoT networks, an attacker can create fake routing nodes, transmission paths, and counterfeit error messages.
- *Access Attack*
  An Access attack occurs when an unauthorized user gains entry to an IoT network, remaining undetected for extended periods. The objective is to clandestinely acquire vulnerable and sensitive data, posing a threat to both the user and the IoT network. Given that IoT devices frequently transfer and receive valuable data, they become highly susceptible to this form of attack [13].
- *DDoS Attack*
  In this attack, an assailant overwhelms a targeted server with substantial traffic, leading to server shutdown and disruption of traffic to customers. While DDoS attacks are not exclusive to IoT devices and applications, many IoT devices have inadequate configurations, making them easy targets for

attackers aiming to bolster their botnet armies. The Mirai botnet notably exploited weakly configured IoT devices as part of its attack.

- *Data Transfer Attack*
  IoT applications involve a significant volume of data in transit, moving across sensors, servers, the cloud, and applications [14]. This complex data transfer, utilizing various technologies, renders IoT applications more susceptible to intrusions. The diverse pathways that data traverses within IoT systems create vulnerabilities that attackers may exploit.

1.3 Application Layer Attacks

Software attacks are executed to gain access to the application layer and illicitly acquire sensitive data. Below are some attacks designed to target data within the application layer:

- *Code and Database Injection Attacks*
  IoT systems may face susceptibility to attacks involving the injection of malicious code [15]. In this scenario, attackers pinpoint vulnerable entry points to insert harmful scripts. By utilizing scripting techniques, these attacks introduce detrimental code into trusted sites and databases. If successful, such an attack can result in unauthorized control of the IoT account, potentially causing harm to the entire IoT network.

- *Theft of Data*
  IoT devices manage valuable data, a significant portion of which is actively transferred. This dynamic data in transit is more susceptible to cyber-attacks compared to data at rest. Users also exhibit greater reluctance to input private information into their IoT devices when they are aware of their vulnerability to potential attacks.

- *Sniffing Attacks*
  Malicious software is employed by attackers to monitor the traffic within IoT networks. This enables them to intercept and read vulnerable data circulating throughout the IoT network [16]. The effectiveness of this attack is heightened in instances where secure data transfer protocols are not implemented, rendering IoT networks susceptible to unauthorized monitoring and data compromise.

- *Phishing Attacks*
  This type of attack occurs when a user is deceived into clicking on emails, browsing web pages, or opening communication messages that masquerade as legitimate sources. The user is typically tricked into accessing links that contain malicious content, such as malware or input fields prompting the user to enter sensitive information. The latter is then illicitly acquired by the assailant.

2. LITERATURE REVIEW

F. Hussain, et.al (2021) investigated a two-stage machine learning (ML) technique for preventing and detecting botnet attacks in Internet of Things (IoT) [17]. Initially, ResNet-18 was implemented for training this technique. Hence, the scanning activity was detected in an advance attack stage for preventing botnet attacks. Subsequently, this technique aimed to train another ResNet-18 model in order

to recognize DDoS attack while detecting botnet assaults. The experimental outcomes revealed that the investigated technique provided an accuracy of 0.9889, precision of 0.9901, recall of 0.9874 and F1-Score of 0.9887 for preventing and detecting IoT botnet assaults. Moreover, 3 diverse datasets were applied for training 3 other ResNet-18 algorithms which detected scan and DDoS attacks. The investigated technique was proved effective for preventing and detecting botnet assaults.

P. M. S. Sánchez, et.al (2023) suggested a Long Short Term Memory-Convolutional Neural Network (LSTM-CNN) model depending upon the hardware performance behavior to recognize individual device [18]. Afterward, the extensive Machine Learning (ML) and Deep Learning (DL) methods were implemented, and the dataset taken from 45 Raspberry Pi devices was executed for computing the suggested model against these methods. The suggested model yielded a F1-Score of 96% and True Positive Rate (TPR) of 0.8. However, some evasion attacks were still found. Thus, adversarial training and model distillation defense (MDD) methods were adopted for making the technique more resistible against evasion attacks at an accuracy of 88% for detecting attacks.

A. K. Dey, et.al (2023) designed a hybrid method of statistical test-based filter (STF) methods, namely Chi-Square ($\chi 2$), Pearson's Correlation Coefficient (PCC), and Mutual Information (MI) and a Non-Dominated Sorting Genetic Algorithm (NSGA-II)-based algorithm to optimize the features [19]. The STF techniques were adopted for assigning ranks to the features to initialize guided population in NSGA-II. Hence, higher convergence speed was attained. The ToN-IoT dataset was considered for quantifying the designed method with respect to selected features and accuracy. According to experiments, the designed method was performed well with least amount of features and offered an accuracy of 99.48%.

R. Harada, et.al (2022) introduced a new suppression system against distributed denial of service (DDoS) attack for mitigating the elimination of authentic traffic using few devices [20]. For this, the priority of frames was controlled in a network which had in Internet of Things (IoT) devices. The simulation exhibited the effectiveness of the introduced system for preventing the authentic traffic in 30 seconds during the occurrence of attack traffic via a traffic generator. Further, Mirai-based DDoS attack traffic was launched to evaluate this system. The findings depicted that the introduced system was capable of blocking attack traffic at the switches when the products of vendors were combined.

X. Liu, et.al (2022) projected a Broad Learning based Comprehensive Defense (BLCD) method in which BL was integrated with a set of defense methods against SSDP attacks [21]. This method was executed with the attack chain for defending against assaults. The projected method was emphasized on detecting suspected traffic at bots, service providers and victims on the basis of BL. The obtained output was considered to implement defense methods for mitigating DDoD packets. An analysis was conducted on the projected method under assault traffic and at diverse defense locations. The experimental outcomes indicated that the projected method was effective for mitigating the number of packets up to 39% and detecting malevolent packets at an accuracy up to 99.99% in comparison with the traditional methods.

N. Nabeel, et.al (2021) constructed a novel Lightweight (LWT) hash function known as Lightweight New Mersenne Number Transform (LNMNT) to secure diverse Internet of Things (IoT) applications [22]. The arbitrariness, confusion, diffusion, distributed hash function, and dissimilar attacks were considered for quantifying the constructed approach. The NIST suit was executed for computing the

randomness. The simulation was conducted on the constructed approach concerning cycles per byte, memory deployment, and consumed energy. The results exhibited the sensitivity against the slight variation in the input message. Moreover, this approach mitigated the execution time, memory consumption and energy deployment as compared to other methods.

E. Gelenbe, et.al (2022) established a new online Compromised Device Identification System (CDIS) for recognizing Internet of Things (IoT) devices infected with a Botnet attack which transmitted the packets [23]. This system aimed to select particular parameters whose extraction was done from network traffic, and training from online model when it was operated normally using an Auto-Associative Dense Random Neural Network (AADRNN) model. The auto-associative learning (ALL) algorithm was employed to train this model based on the traffic for estimating it as benign, without gathering the attack data. MIRAI dataset was executed for simulating the established system. The experimental outcomes revealed that the established system had detected the botnet attack at an accuracy of 97%. The utilized model was performed well in contrast to 6 diverse techniques. Moreover, the established system was robust for preventing the IoT network from the spread of Botnet attacks.

J. Roldán-Gómez, et.al (2023) developed an innovative framework to formulate Complex Event Processing (CEP) rules automatically when machine learning (ML) methods were incorporated [24]. The initial one was assisted in detecting attack patterns in real time and the Principal Component Analysis (PCA) algorithm was employed for characterizing events and recognizing anomalies in Internet of Things (IoT). The formulated rules were assisted in enhancing the traditional rules. According to experiments, the developed framework had detected the attack at F1-score up to 98% and throughput of 76%, and mitigated the overhead up to 86%.

S. Cakir, et.al (2020) recommended a Gated Recurrent Unit (GRU) network based deep learning (DL) for predicting and preventing Hello Flooding (HF) assaults on RPL protocol in Internet of Things (IoT) networks [25]. A comparative analysis was conducted on the recommended approach against Support Vector Machine (SVM) and Logistic Regression (LR) methods concerning power states and power usage. The experimental outcomes confirmed the supremacy of the recommended approach for securing the IoT network and making it source effective. Besides, this approach detected the attack at 99.96% accuracy and offered least error rate (ER) in contrast to the conventional methods.

X. Zhou, et.al (2022) intended a new hierarchical adversarial attack (HAA) generation technique for executing level-aware black-box adversarial attack (ABAA) method on the basis of graph neural network (GNN)-based method of detecting intrusion in Internet of Things (IoT) systems [26]. A shadow GNN algorithm planned on the basis of a saliency map was put forward for creating instances of adversarial instances, when the crucial feature components were recognized and modified at least perturbations. A random walk with restart (RWR)-based hierarchical algorithm was generated for selecting a set of more vulnerable nodes having higher attack priority. The UNSW-SOSR2019 dataset was applied to compute the intended technique. The experimental results depicted that the intended technique was robust as compared to the traditional methods.

A. Liu, et.al (2021) formulated IoTVerif model for automatically determining the Secure Socket Layer/Transport Layer Security (SSL/TLS) certificate for Internet of Things (IoT) applications in which broker-based messaging protocols were deployed [27]. The major objective was to generate the specification of an IoT protocol and verify its security properties. Afterward, a general-purpose checker

was executed for determining those properties and producing counter-examples in case of failure of any property. The real-time applications were applied to simulate the formulated model. The findings revealed that the formulated model was feasible for recognizing susceptibilities from IoT applications under man-in-the-middle (MITM) and TLS renegotiation attacks.

X. Tao, et.al (2023) suggested an encryption method known as lattice-based matchmaking identity-based encryption (LMIBE) which allowed bilateral access control to sender and receiver in Internet of Things (IoT) systems, and was resistible against quantum attacks [28]. This system facilitated the receiver in recognizing the ciphertexts from illegal senders at lower cost for decrypting data. Besides, an enormous workload of authentication was outsourced to sanitizer for preventing the dangerous information via messages and lessening the burden of incurable equipment. The suggested method was computed in experiments. The results indicated the security and robustness of the suggested method against diverse assaults.

3. RESEARCH METHODOLOGY

The IoT traffic classification models will help us to identify type of traffic in the network. The IoT traffic classification models have various steps which include data set pre-processing, feature extraction, classification and performance analysis. The various schemes are proposed in the past years for the efficient network traffic classification. The existing schemes has various drawbacks which we need to entertain in the research work. The KDD dataset is very large in size due to which existing schemes are unable to establish relation of each attribute with target set. In this research work, the novel scheme will be proposed which can extract features of the dataset for the efficient classification. The hybrid classification models will be proposed which will improve performance for the IoT traffic classification. The motivation of this research work is to increase accuracy and methodology is described below: -

3.1 Data set input and Pre-processing

The initial stage is the dataset input in which data gathered from the genuine source named KDD is utilized for input. This study employs a NSL-KDD dataset in which 42 attributes are compromised. The duplicate instances are eliminated to enhance the KDD’99 datasets with the purpose of removing the biased classification results from the dataset. The utilization of only 20% of training data is done. However, various editions of the data set are present. This data is represented in the form of KDDTrain+_20Percent.

3.2 Feature Extraction

The feature extraction is the important phases in which relationship between attribute set and target set is established. The hybrid optimization algorithm is the combination of genetic and PSO algorithm. The proposed flowchart is the hybrid version of Genetic and PSO algorithm. This algorithm is useful to select the optimization attributes and encoding an effective solution for an issue into an individual. In fact, every individual is considered as an entity supporting features of chromosomes. A number of individuals collectively creates a population. The major task is to generate a population of chromosomes randomly and surround it with variables of problem prior to deploy Genetic Algorithm (GA). The next phase emphasizes on assessing the created data chromosomes. The chromosomes, which are capable of clearly demonstrating an optimal method for tackling the issue, are useful for building other chromosomes. The population is defined as the primary set of random solutions available in this

algorithm. A chromosome is utilized for illustrating every member of the population in order to perform coding for a solution for dealing with the issue. The decoding formula is expressed as:

$$X = X_{min} + \frac{X_{max} - X_{min}}{2^{Nx} - 1} \sum_{n=0}^{N^x - 1} b_n^X 2^n \quad (6)$$

In which, $b_0^X, \ldots\ldots, b_{N^x-1}^X$ denote the binary representations of X's. Various iterations called generations are exploited for creating the chromosomes. In every generation, a number of fitness indicators are executed for evaluating the fitness value of the chromosomes. Every particle i has a relation with 2 vectors, such as the position vector denoted with $\boldsymbol{X}_i = [x_{i,1}, x_{i,2}, \ldots, x_{i,n}]$ and the velocity vector $\boldsymbol{V}_i = [v_{i,1}, v_{i,2}, \ldots, v_{i,n}]$. The positions $x_{i,d}$of novel solutions are adjusted at constant rate for performing their searching process. For every particle, this algorithm focuses on reminding the historical location of an individual as $\boldsymbol{pbest}_i$, and the current global optimal position which the entire particle swarm has discovered is defined with $\boldsymbol{gbest}$. The discovery of these locations lead to update the velocity and position of every particle in according with the given equations as:

$$v_{i,d}(t+1) = \omega \cdot v_{i,d}(t) + c_1 \cdot rand_1 \cdot \left(\boldsymbol{pbest}_{i,d} - x_{i,d}(t)\right) + c_2 \cdot rand_2 \cdot \left(\boldsymbol{gbest}_d - x_{i,d}(t)\right) \quad (7)$$

$$x_{i,d}(t+1) = x_{i,d}(t) + v_{i,d}(t+1) \quad (8)$$

In this, the t-th iteration is illustrated with t, d is used to represent the d-th dimension of the particle, ω denotes the inertia weight, c_1 and c_2 are used to demonstrate the acceleration constants, the random numbers are specified with $rand_1$ and $rand_2$ whose distribution is done at random within the interval [0, 1]. The mitigation of the inertia weight ω leads to enhance the efficiency of this algorithm. this weight is defined as:

$$\omega = \omega_{max} - (\omega_{max} - \omega_{min}) \cdot \frac{t}{t_{max}} \quad (9)$$

In this, ω_{max} is used to denote the maximal weight and ω_{min} shows the minimum weight, t defines the number of the current iteration, and the number of the maximum iteration is specified with t_{max}. The crossover operator or a mutation operator (MO) are implemented to integrate 2 chromosomes taken from the current generation for generating the offspring. A steady population size is maintained through an innovative generation. Some parents and children are selected on the basis of fitness values and others are rejected for producing this generation. Several possibilities are available for fitter chromosomes.

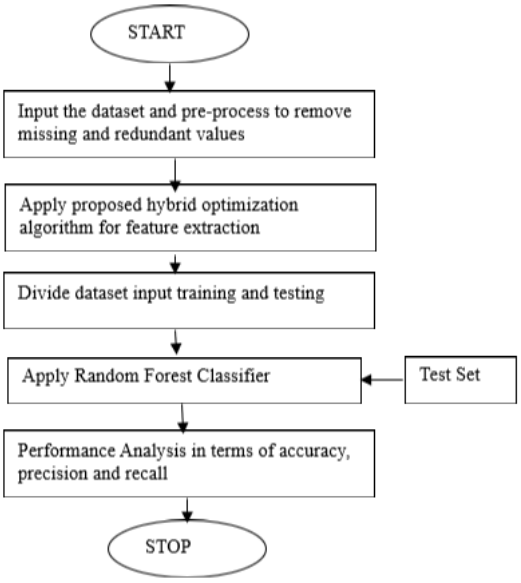
3.3 Classification

The random forest classifier is applied for the classification. The random forest model takes out of optimization algorithm as input for the classification. In Random Forest the trees are combined to create a single, strong learner after averaging or getting the majority vote when numerous tiny, weak DTs are formed in tandem. The RFs are frequently studied as the most precise learning algorithms for training to date. Formally, an RF be a predictor built of a set of randomly generated base regression trees, where $\{r_n(x, \ominus_m, D_n), m \geq 1\}, where\ \ominus_1, \ominus_2$ .... are the independently distributed outputs of a randomly generated variable $\ominus$. For the purpose of creating the aggregated regression estimate, these RT integrations are performed.

$$\bar{r}_n(X, D_n) = \mathbb{E}_{\ominus}[r_n(X, \ominus, D_n)], \quad (10)$$

In where, subject to X and the data set D_n, $\mathbb{E}_{\ominus}$ denotes what is expected as a function of the random parameter. The dependence of the estimations would be eliminated from the sample in the following notation to simplify it a little and given in the form $\bar{r}_n(X)$ rather than $\bar{r}_n(X, D_n)$. When the M RTs are generated and the average of the individual outcomes is obtained, Monte Carlo was used to calculate the aforementioned expectation. When creating individual trees, where the choice of the split coordinate and split position are constructed, the randomising variable $\ominus$ is used to assess how well subsequent cuts work. As the independent of X and the training sample D_n, the variable $\ominus$ is inferred.

4. FLOW CHART



Model	Accuracy	Precision	Recall
SVM Classifier	75.74 Percent	81 Percent	76 Percent
Logistic Regression	72.67 Percent	80 Percent	77 Percent
KNN Classifier	70 Percent	72 Percent	76 Percent
Random Forest Classifier	75.78 Percent	76.89 Percent	75.90 Percent

Figure 2: Proposed Model

5. RESULT AND DISCUSSION

In this section includes results of the proposed model which is compared with existing models for the intrusion detection in IoT. In the Below sections dataset details with results are elaborated.

5.1. Dataset Description

The KDD 99 intrusion detection datasets are based on the 1998 DARPA initiative to provide designers of intrusion detection systems (IDS) with a benchmark on which to evaluate different methodologies. To do so, a simulation is made of a factitious military network consisting of three ‘target’ machines running various operating systems and services. Additional three machines are then used to spoof different IP addresses, thus generating traffic between different IP addresses. Finally, there is a sniffer

that records all network traffic using the TCP dump format. The total simulated period is seven weeks. Normal connections are created to profile that expected in a military network and attacks fall into one of four categories: User to Root; Remote to Local; Denial of Service; and Probe. • Denial of Service (dos): Attacker tries to prevent legitimate users from using a service. • Remote to Local (r2l): Attacker does not have an account on the victim machine, hence tries to gain access. • User to Root (u2r): Attacker has local access to the victim machine and tries to gain super user privileges. • Probe: Attacker tries to gain information about the target host. In 1999, the original TCP dump files were pre-processed for utilization in the Intrusion Detection System benchmark of the International Knowledge Discovery and Data Mining Tools Competition. To do so, packet information in the TCP dump file is summarized into connections. Specifically, "a connection is a sequence of TCP packets starting and ending at some well-defined times, between which data flows from a source IP address to a target IP address under some well-defined protocol.

5.2. Results

This research work is conducted on the basis of classifying the network traffic. The framework of classifying the network traffic classification is executed in diverse phases in which the data is pre-processed, features are extracted and the data is classified. The dataset which is used for the model testing is of KDD. The KDD dataset has the 42 attributes and target set which contain multiple classes of different attacks. Various metrics such as accuracy, precision and recall are considered to evaluate the introduced technique. The Classification implemented for the network traffic classification of IoT. The SVM, KNN, Logistic Regression and Random Forest is implemented for the IoT network traffic classification. The results of the classification algorithm is described in table 1.

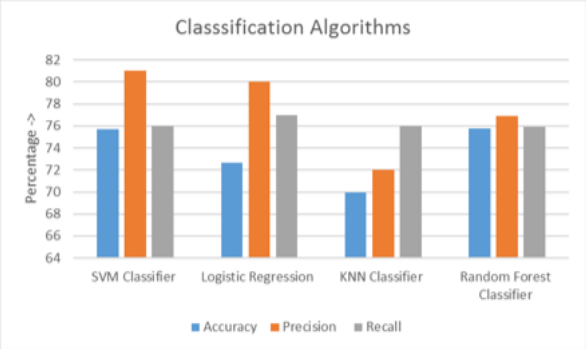


Figure 2: Classification Algorithms Results

As shown in figure 2, various classification algorithms like SVM, Logistic regression, KNN and Random forest is implemented for the classification of IoT Data. The maximum accuracy is achieved by the random forest algorithm which is 75.78 percent, the precision value of SVM is maximum which is 81 percent and recall of logistic regression is maximum with 77 percent.

Models	Accuracy	Precision	Recall
Gray Wolf+ Random Forest	73.88 Percent	81 Percent	74 Percent
BAT +Random Forest	76.64 Percent	82 Percent	77 Percent
Firefly+ Random Forest	77.36 Percent	77 Percent	74 Percent
PSO+ Genetic+ Random Forest	99.76 Percent	99 Percent	99 Percent

Table 1: Optimization Algorithm Results

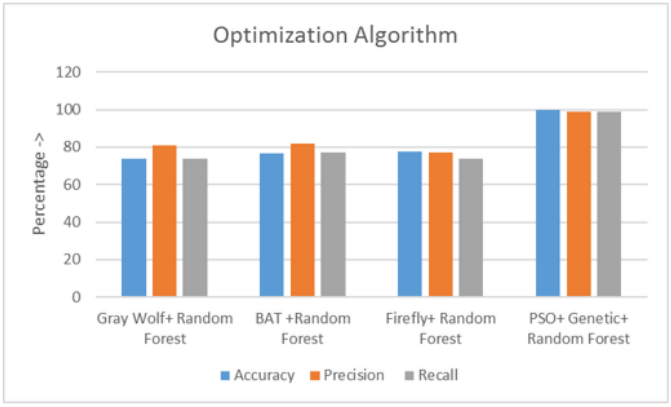


Figure 3: Results of Optimization with Random Forest Classifier

As shown in figure 3, the results of various optimization algorithm with random forest classifier is shown in trms of accuracy, precision and recall. The Gray Wolf, BAT, Firefly and proposed hybrid optimization algorithm is implemented for the IOT network traffic classification. The maximum accuracy, precision and recall is achieved by proposed hybrid optimization algorithm as compared to Gray wolf, BAT and firefly algorithm.

CONCLUSION

In this paper, it is concluded that Internet of things network is much vulnerable for the security attacks. The various type of attacks is the possible in the network which can be named as DOS, Reply, Version number etc. The machine learning algorithms is the most advance algorithms which can be used for the classification of the attacks from the network. The machine learning algorithms which are proposed in the past years is unable to achieve good accuracy due to loop hole in feature extraction phase. The hybrid optimization algorithm is proposed for the feature extraction which is the combination of PSO and genetic algorithm. The various other optimization algorithms like Gray wolf, BAT and Firefly are also applied for the feature extraction. The proposed algorithm is implemented in python and results is also compared with machine learning algorithms like SVM, BAT and firefly. The proposed model achieve accuracy, precision and recall of 99 percent IOT network traffic classification. The results of the proposed model are 30 to 35 percent high as compared machine learning algorithm and also to other optimization algorithms. In future deep learning models can be applied for the IOT network traffic classification.

REFERENCES

[1] J. R. Elias, R. Chard, J. A. Libera, I. Foster and S. Chaudhuri, "The Manufacturing Data and Machine Learning Platform: Enabling Real-time Monitoring and Control of Scientific Experiments via IoT," 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, pp. 1-2, 2020.

[2] S. S. Swarna Sugi and S. R. Ratna, "Investigation of Machine Learning Techniques in Intrusion Detection System for IoT Network," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, pp. 1164-1167,2020.

[3] M. Afroz, N. Hasan and M. I. A. Hossain, "IoT Based Two Way Safety Enabled Intelligent Stove with Age Verification Using Machine Learning," 2021 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, pp. 1-5,2021.

[4] N. Karmous, M. O. -E. Aoueileyine, M. Abdelkader and N. Youssef, "IoT Real-Time Attacks Classification Framework Using Machine Learning," 2022 IEEE Ninth International Conference on Communications and Networking (ComNet), Hammamet, Tunisia, pp. 1-5,2022.

[5] H. Pandey and S. Prabha, "Smart Health Monitoring System using IOT and Machine Learning Techniques," 2020 Sixth International Conference on Bio Signals, Images, and Instrumentation (ICBSII), Chennai, India, pp. 1-4,2020.

[6] S. M. Shahriar, H. I. Peyal, M. Nahiduzzaman and M. A. H. Pramanik, "An IoT-Based Real-Time Intelligent Irrigation System using Machine Learning," 2021 13th International Conference on Information & Communication Technology and System (ICTS), Surabaya, Indonesia, pp. 277-281,2021.

[7] U. Arul, A. A. Prasath, S. Mishra and J. Shirisha, "IoT and Machine Learning Technology based Smart Shopping System," 2022 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS), Chennai, India, pp. 1-3,2022.

[8] V. T. Hayashi et al., "Improving IoT Module Testability with Test-Driven Development and Machine Learning," 2021 8th International Conference on Future Internet of Things and Cloud (FiCloud), Rome, Italy, pp. 406-412,2021.

[9] S. Kavitha, V. R. Karumanchi, T. S. Rajeswari, V. C. Jadala, S. H. Raju and M. Kavitha, "Machine Learning based Authentication of loT Devices in Traffic Prediction for ITS," 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, pp. 1530-1534,2022.

[10] Z. Liu, N. Thapa, A. Shaver, K. Roy, X. Yuan and S. Khorsandroo, "Anomaly Detection on IoT Network Intrusion Using Machine Learning," 2020 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD), Durban, South Africa, pp. 1-5,2020.

[11] M. Bagaa, T. Taleb, J. B. Bernabe and A. Skarmeta, "A Machine Learning Security Framework for Iot Systems," in IEEE Access, vol. 8, pp. 114066-114077, 2020.

[12] H. Lee, S. Kim, D. Baek, D. Kim and D. Hwang, "Robust IoT Malware Detection and Classification Using Opcode Category Features on Machine Learning," in IEEE Access, vol. 11, pp. 18855-18867, 2023.

[13] W. Ma, X. Wang, M. Hu and Q. Zhou, "Machine Learning Empowered Trust Evaluation Method for IoT Devices," in IEEE Access, vol. 9, pp. 65066-65077, 2021.

[14] T. Gaber, A. El-Ghamry and A. E. Hassanien, “Injection attack detection using machine learning for smart IoT applications”, Physical Communication, vol. 173, no. 4, pp. 5363-5365, 16 March 2022.

[15] D. Mishra, B. Naik and S. Vimal, “Light gradient boosting machine with optimized hyperparameters for identification of malicious access in IoT network”, Digital Communications and Networks, vol. 9, no. 1, pp. 125-137, 12 October 2022.

[16] R. Banavathu and S. Meruva, “Efficient secure data storage based on novel blockchain model over IoT-based smart computing systems”, Measurement: Sensors, 10 March 2023.

[17] F. Hussain et al., "A Two-Fold Machine Learning Approach to Prevent and Detect IoT Botnet Attacks," in IEEE Access, vol. 9, pp. 163412-163430, 2021, doi: 10.1109/ACCESS.2021.3131014.

[18] P. M. S. Sánchez, A. H. Celdrán and G. M. Pérez, “Adversarial attacks and defenses on ML- and hardware-based IoT device fingerprinting and identification”, Future Generation Computer Systems, vol. 152, pp. 30-42, doi: 10.1016/j.future.2023.10.011, 27 October 2023.

[19] A. K. Dey, G. P. Gupta and S. P. Sahu, “Hybrid Meta-Heuristic based Feature Selection Mechanism for Cyber-Attack Detection in IoT-enabled Networks”, Procedia Computer Science, vol. 218, pp. 318-327, doi: 10.1016/j.procs.2023.01.014, 31 January 2023.

[20] R. Harada et al., "Quick Suppression of DDoS Attacks by Frame Priority Control in IoT Backhaul with Construction of Mirai-Based Attacks," in IEEE Access, vol. 10, pp. 22392-22399,

doi: 10.1109/ACCESS.2022.3153067, 2022.

[21] X. Liu, L. Zheng and J. Zhou, “A broad learning-based comprehensive defence against SSDP reflection attacks in IoTs”, Digital Communications and Networks, vol. 9, no. 5, pp. 1180-1189, doi:10.1016/j.dcan.2022.02.008, 2 March 2022.

[22] N. Nabeel, M. H. Habaebi and M. D. R. Islam, "Security Analysis of LNMNT-LightWeight Crypto Hash Function for IoT," in IEEE Access, vol. 9, pp. 165754-165765, doi: 10.1109/ACCESS.2021.3133097,2021.

[23] E. Gelenbe and M. Nakıp, "Traffic Based Sequential Learning During Botnet Attacks to Identify Compromised IoT Devices," in IEEE Access, vol. 10, pp. 126536-126549, doi: 10.1109/ACCESS.2022.3226700, 2022.

[24] J. Roldán-Gómez, J. Boubeta-Puig and J. M. del Rincón, “An automatic complex event processing rules generation system for the recognition of real-time IoT attack patterns”, Engineering Applications of Artificial Intelligence, vol. 123, pp. 38-45, doi: 10.1016/j.engappai.2023.106344, 28 April 2023.

[25] S. Cakir, S. Toklu and N. Yalcin, "RPL Attack Detection and Prevention in the Internet of Things Networks Using a GRU Based Deep Learning," in IEEE Access, vol. 8, pp. 183678-183689, doi:10.1109/ACCESS.2020.3029191, 2020.

[26] X. Zhou, W. Liang, W. Li, K. Yan, S. Shimizu and K. I. -K. Wang, "Hierarchical Adversarial Attacks Against Graph-Neural-Network-Based IoT Network Intrusion Detection System," in IEEE Internet of Things Journal, vol. 9, no. 12, pp. 9310-9319, doi: 10.1109/JIOT.2021.3130434, 15 June, 2022.

[27] A. Liu, A. Alqazzaz, H. Ming and B. Dharmalingam, "Iotverif: Automatic Verification of SSL/TLS Certificate for IoT Applications," in IEEE Access, vol. 9, pp. 27038-27050, doi: 10.1109/ACCESS.2019.2961918, 2021.

[28] X. Tao, Y. Qiang, P. Wang and Y. Wang, "LMIBE: Lattice-Based Matchmaking Identity-Based Encryption for Internet of Things," in IEEE Access, vol. 11, pp. 9851-9858, doi: 10.1109/ACCESS.2023.3240304, 2023.