Tuijin Jishu/Journal of Propulsion Technology
ISSN:1001-4055
Vol. 44 No.6(2023)

Analysis of Attack Detection Using Various Techniques over Internet of Things

Mrs. B. Dhivya[1], Dr. S. Thavamani[2]

[1]Research Scholar(Part-time) in Computer Science and Assistant Professor, Department of Computer Science, Sri Ramakrishna College of Arts & Science(Autonomous), Coimbatore, Tamil Nadu, India.
[2]Associate Professor, Department of Computer Applications, Sri Ramakrishna College of Arts & Science(Autonomous), Coimbatore, Tamil Nadu, India.

Abstract: Internet of Things (IoT) has become one of the fastest-growing technologies and has been broadly applied in various fields. IoT, networks contain millions of devices with the capability of interacting with each other and providing functionalities that were never available to us before. These IoT networks are designed to provide friendly and intelligent operations through big data analysis of information generated or collected from an abundance of devices in real time. However, the diversity of IoT devices makes the IoTenvironments more complex and more vulnerable to various attacks compared to traditional computer networks.Hence, the misclassification error rate, accuracy and computational complexity are main issues for the given datasets. To overcome these issues, the existing methods are analyzed various techniques of swarm intelligence algorithms and classification methods which can be applied to bring out hidden knowledge from the specified dataset. There are different methods available for classification of attack detection dataset which is divided into three main categories, attack detection on IoT, swarm intelligence algorithms for attack detection and classification. Each of this technique has their own advantages and disadvantage. The comparative analysis evaluated on the basis of accuracy percentage on the application of various classification techniques like Software-defined network (SDN)-Fuzzy Neural Network (FNN), Random Neural Network (RNN), Hybrid Deep Learning based Convolutional Neural Network -Adaptive Neuro-Fuzzy Inference System (IFFO-HDLCNN + ANFIS) andTunicate Swarm Algorithm (TSA)-Long Short-Term Memory-Recurrent Neural Network (LSTMRNN) model approaches. The experimental result shows that the TSA-LSTMRNN algorithm provides better performance in terms of higher accuracy, precision, recall and f-measure rather than the other existing methods.

Keywords*: Internet of Things (IoT), attack detection, pre-processing, swarm intelligence algorithm,classification.*

1. Introduction

As one of the fastest-growing and widely used technologies on the Internet, IoT extends the edge of the Internet by connecting additional terminal devices and facilities on the edge of the network. Specifically, IoT contains millions of devices with the capability of interacting with each other and providing great convenience. Incredible developments in the routine use of electronic services and applications have led to massive advances in telecommunications networks and the emergence of the concept of the IoT[1]. The IoT is an emerging communications paradigm in which devices serve as objects or “things” that have the ability to sense their environment, connect with each other, and exchange data over the Internet.

Via IoT technology, smart cities, smart home, smart medical treatment, smart agriculture, and other smart fields are emerging.The goal of developing such smart environments is to make human life more productive and comfortable by solving challenges related to the living environment energy consumption, and industrial needs [2] [3]. This goal is directly reflected in the substantial growth in the available IoT-based services and applications across different networks. There are millions of IoT devices all over the world, some of which are visible while others are not. The data collected from these devices and stored in datacenters contain vast amounts of

information, which may contain individuals' private information. More visible and invisible threats are emerging and causing irrecoverable damages.

Due to the high concentration of various information, attackers often select storage and service servers as a primary attack target. Once the attackers gain access to the central severs, data breaches are inevitable. Furthermore, the local storage and computing limitations of IoT devices prevent them from detecting and defending against potential attacks[4]. A minor security threat has the potential to cause severe damage to IoT networks. Therefore, there is no doubt that ensuring the security of IoT networks is of great significance to the success of IoT applications. Compared with traditional computer networks, there are more terminal devices and traffic in IoT networks, which make IoT network security issues more complex and troublesome.

Feature Selection (FS) algorithms are introduced for selecting the most informative features from the original input data. FS is of substantial prominence in attack detection which is potent in augmenting learning efficacy, increasing generalization effect, and achieving data visualization. In the case of feature selection, a feature containing important information about a class is considered as relevant, while the irrelevant feature holds little information about the output class and can be known as uninformative features to the output class [5]. The key point solving the problems is to search for those informative features that contain as much information about the output class as possible.

Classification is the process of predicting the categorical labels. It is used to classify the data based on the training set and the values in a classifying attribute. Classification is also known as class prediction, discriminant analysis, or supervised learning. Classification model used to predict class labels and testing the constructed model on test data and hence estimate the accuracy of the classification rules. Machine Learning (ML) and Deep Learning (DL) techniques are used to monitor and analyze large amount of network data and classify these network data into anomalous and normal data [6] [7]. Since data comes from various sources, network traffic is large. DL technique is applied to build attack detection model efficiently.

The main problem of this research work is the attack detection in IoT environment. There are several research and methodologies introduced but the attack detection accuracy is not achieved significantly. The existing approaches has drawback with computational overhead and inaccurate attack classification results. Therefore, this survey study suggests that the pre-processing, feature selection and classification. So, the comprehensive survey study mainly focused on attack detection accuracy performance by using efficient and effective methods

The rest of the paper is organized as follows: a brief review of some of the literature works in pre-processing, feature selection and classification are presented in Section 2. The research gap is discussed in Section 3. Finally, section 4 defines the experimental result and section 5 provides conclusion of the survey study.

2. Related Work

There are various approaches presented by different authors for pre-processing, feature selection and classification process. This section discusses the current and most frequently used techniques of research published in recent times.

2.1 Review on attack detection methods in IoT

In [8], Baydoğmuş and GözdeKarataş (2021) discussed the importance of normalization and standardization in data preprocessingwhich is examined to make machine learning approaches more successful for detecting attacks on IoT devices. The study is carried out in Logistic Regression, Decision Tree, and Stochastic Gradient Descent machine learning algorithms using the Bot-IoT dataset. Bot-IoT dataset is a popular dataset that is widely used in security studies on IoT devices. Normalization and standardization processes were applied to Bot-IoT dataset separately, so data preprocessingis performed, then selected machine learning algorithms were trained with these normalized / standardized datasets. As a result of the trainings made with machine learning algorithms, the values of Accuracy, Precision, Recall and F1 Score rates were examined.

In [9], Karthik, M. Ganesh, and MB Mukesh Krishnan (2021) introduced new model based on random forest and synthetic minority over-sampling technique (RF-SMOTE) to detect the attacks in an IoT network. In this research, the experimental analysis is performed for IoT attack detection, where the evaluation is done on NSL-KDD dataset and network-based detection of IoT (N-BaIoT) dataset, which are the well-known datasets for IoT

attack detection. In the experimental phase, the RF-SMOTE model showed minimum of 0.14% and maximum of 14.25% improvement in accuracy on NSL-KDD dataset for binary class. In addition, the model averagely showed minimum of 0.04% and maximum of 7.35% improvement in accuracy on NSL-KDD dataset for four classes.

In [10], Muthanna et al (2022) aims for efficient threat detection in IoT environments using an intelligent, SDN-enabled hybrid framework leveraging Cuda Long Short Term Memory Gated Recurrent Unit (cuLSTMGRU). To properly assess the system, a state-of-the-art IoT-based dataset and standard evaluation metrics are used. The model achieved better detection accuracy with a low false-positive rate. The model outclassed the other models regarding speed efficiency, detection accuracy, precision, and other standard evaluation metrics. Finally, the work employed 10-fold cross-validation to ensure that the results were completely unbiased.

In [11], Roy et al (2022) suggested novel intrusion detection model that uses machine learning to effectively detect cyber-attacks and anomalies in resource-constraint IoT networks. Through a set of optimizations including removal of multicollinearity, sampling, and dimensionality reduction, our model can identify the most important features to detect intrusions using much fewer training data and less training time. Extensive experiments were performed on the CICIDS2017 and NSL-KDD datasets respectively to evaluate the approach. The experimental results on two popular datasets show that our model has a high detection rate and a low false alarm rate. It outperforms existing models in multiple performance metrics and is consistent in classifying major cyber-attacks, respectively. Most importantly, unlike traditional resource-intensive intrusion detection systems, the model is lightweight and can be deployed on IoT nodes with limited power and storage capabilities.

In [12], Reddy et al (2021) presented a security mechanism and assure truthful operation of IoT networks with the intrusion detection system. A network intrusion detection system is used based on the conception of the Exact Greedy Boosting ensemble method for device implementation in the fog node because of protecting critical infrastructure from timely and accurate detection of malicious activities. The model explores the traffic flow monitoring in novel IoT Intrusion Dataset 2020(IoTID20) network traffic by identifying and classifying the type of attack based on anomalies from normal behavior. Further, the paper estimates the complete experimentation performance and evaluations with competitive machine learning algorithms. The experimental observation Table 1 of the simulation work is evident in the model's efficiency and robustness in categorizing the attacks.

Table 1. Inference of Existing Attack Detection Methods in IoT.

S.No	Methods	Merits	Demerits	Parameters improved
1	Normalization and standardization [8]	This approach increases the features available to each class Higher accuracy	It does not take into consideration neighboring examples can be from other classes.	It is seen that the standardization increased the accuracy rate up to 99.96% in Logistic Regression.
2	RF-SMOTE [9]	Computational complexity is reduced significantly It provides greater accuracy in detecting attacks	For large dataset, classification performance is low It requires higher memory	This model averagely showed minimum of 0.04% and maximum of 7.35% improvement in accuracy on NSL-KDD dataset for four classes
3	SDN-enabled hybrid framework [10]	It avoids setting free parameters over IoT It is more effective in high dimensional spaces	Long training time for large dataset In few cases system efficiency is reduced	This model achieved 99.23%detection accuracy with a low false-positive rate.
4	Machine learning[11]	It helps to overcome	It does not suitable	It ensured the accuracy with

		the overfitting problem It discards irrelevant attributes from the given dataset	for high dimensional dataset	99.11%
5	Greedy Boosting ensemble method[12]	It provides higher accuracy, sensitivity, specificity and precision This model has efficiency and robustness in categorizing the attacks	However, it has problem with expensive rates	It ensures the sensitivity by 75%

2.2 Review on swarm intelligence methods for attack detection in IoT

In [13], Keserwani et al (2021) discussed Intrusion Detection System (IDS) to identify various attacks for IoT networks. A combination of Grey Wolf Optimization (GWO) and Particle Swarm Optimization (PSO) is used to extract relevant IoT network features. The extracted features are fed to a random forest (RF) classifier to achieve high attack detection accuracy. The experiments are conducted in the python programming environment to evaluate the model on KDDCup99, NSL–KDD, and CICIDS-2017 datasets. The GWO–PSO–RF NIDS model has achieved better accuracy for multiclass classification. The accuracy of the model has been compared with other similar approaches to show its effectiveness. The work presented here also addresses the issue of data imbalance.

In [14], Liu et al (2021) introduced PSO-based gradient descent (PSO-LightGBM) for the intrusion detection. In this method, PSO-LightGBM is used to extract the features of the data and inputs it into one-class SVM (OCSVM) to discover and identify malicious data. The UNSW-NB15 dataset is applied to verify the intrusion detection model. The experimental results show that the model is very robust in detecting either normal or various malicious data, especially small sample data such as Backdoor, Shellcode and Worms.

In [15], Krishna et al (2021) suggested hybrid optimization approach using a hybrid Metaheuristic lion optimization algorithm and Firefly optimization algorithm (ML-F) is used. The NSL-KDD and NBaIoT datasets are used where the input data is pre-processed to remove the noises and the missing data. After preprocessing the data, feature extraction is undergone using Recursive feature elimination (RFE).The low rate attacks are selected after splitting the data using a hybrid ML-F optimization algorithm. After selecting the features,a random forest classifier is used for the process of classifying the attacks. The hybrid ML-F method achieves higher performance than the existing gradient boost classifier method in classifying the attacks. The hybrid ML-F method achieved an accuracy, precision, recall and f-measure.

In [16], Li et al (2022) employedartificial neural network to detect abnormal behavior in a medical IoT system. The accuracy of the detection depends heavily on the features that are fed into the artificial neural network. Selecting the important and discriminative features of network traffic is a crucial and challenging issue because it has a significant impact on the learning process. In this work, the butterfly optimization algorithm which is a meta-heuristic optimization algorithm is employed to select the optimal features for the learning process in an artificial neural network. The results achieved, 93.27% accuracy, indicate the capability of the butterfly optimization algorithm to determine discriminative features of network traffic data. The algorithm outperformed the decision tree, support vector machine, and ant colony optimization, which isused in previous researches for the same goal.

In [17], Alharbi et al (2021) adopted Local-Global Best Bat Algorithm for Neural Networks (LGBA-NN) to select both feature subsets and hyperparameters for efficient detection of botnet attacks, inferred from 9 commercial IoT devices infected by two botnets: Gafgyt and Mirai. The Bat Algorithm (BA) adopted the local-

global best-based inertia weight to update the bat's velocity in the swarm. To tackle with swarm diversity of BA, Gaussian distribution used in the population initialization. Furthermore, the local search mechanism is followed by the Gaussian density function and local-global best function to achieve better exploration during each generation. Enhanced BA is further employed for neural network hyperparameter tuning and weight optimization to classify ten different botnet attacks with an additional one benign target class. The LGBA-NN algorithm is tested on an N-BaIoT data set with extensive real traffic data with benign and malicious target classes. The performance of LGBA-NN is compared with several recent advanced approaches such as weight optimization using Particle Swarm Optimization (PSO-NN) and BA-NN. The experimental results revealed the superiority of LGBA-NN with 90% accuracy over other variants, i.e., BA-NN (85.5% accuracy) and PSO-NN (85.2% accuracy) in multi-class botnet attack detection.

In [18], Stankovic et al (2022) suggests hybrid variant of Artificial Bee Colony (ABC) metaheuristics to tackle the feature selection, aiming to increase the accuracy of the extreme learning machine classifier. The novel model has been validated on two famous network security datasets (UNSW-NB15 and CICIDS-2017) to demonstrate the improvement in the performances, and the simulation outcomes were compared to the results obtained by other contemporary methods that have been employed for the same task and under similar circumstances.

In [19], Zhang et al (2019) presents an intrusion detection model based on improved Genetic Algorithm (GA) and Deep Belief Network (DBN). Facing different types of attacks, through multiple iterations of the GA, the optimal number of hidden layers and number of neurons in each layer are generated adaptively, so that the intrusion detection model based on the DBN achieves a high detection rate with a compact structure. Finally, the NSL-KDD dataset is used to simulate and evaluate the model and algorithms. The experimental results show that the improved intrusion detection model combined with DBN can effectively improve the recognition rate of intrusion attacks and reduce the complexity of the neural network structure.

In [20], Gupta et al (2022) introduced novel malware detection framework based on machine learning in IoT using a Genetic Cascaded Support Vector Machine (GC-SVM) classifier. We introduce the Chaotic Binary Coded Cuckoo Search Optimization Algorithm (CBC-CSOA) for optimizing the detection process. The performance of the method is evaluated and compared with various conventional methodologies. The method produced accurate outputs this approach may be used to forecast and identify malware in IoT-based systems. Refer Table 2.

Table 2. Inference of Exiting Swarm Intelligence Method for Attack Detection in IoT.

S.No	Methods	Merits	Demerits	Parameters improved
1	Grey Wolf Optimization (GWO) and Particle Swarm Optimization (PSO) [13]	The GWO–PSO–RF NIDS model has achieved better accuracy for multiclass classification It reduces overfitting problem	Once a feature is eliminated from the model it is not re-entered again However, a dropped variable may become significant later in the final model	The GWO–PSO–RF NIDS model has achieved an average accuracy of 99.66% for multiclass classification
2	PSO-LightGBM[14]	It is very robust in detecting either normal or various malicious data, especially small sample data such as Backdoor, Shellcode and Worms	It is slower for computation	PSO-LightGBM not only does not reduce the detection ability of high frequency data, but greatly increases the detection rate of Backdoor, Shellcode and Worms to reach 51.28%, 64.47% and 77.78%, respectively

		It provides more accurate results for attack classification in IoT		
3	Hybrid Metaheuristic lion optimization algorithm and Firefly optimization algorithm (ML-F) [15]	This algorithm improves both the stability and the accuracy It provides both local and global optimal features The hybrid ML-F method achieved better accuracy, precision, recall and f-measure	Lower convergence rate In few cases, it leads computational complexity	The hybrid ML-F method achieved an accuracy of 99.98%, precision of 99.87%, recall of 100% and f-measure of 99.73%. The existing gradient boosting classifier method shows the Accuracy of 50.93%, Precision of 54.87%, Recall of 77.67% and F-measure of 64.34%
4	Butterfly optimization algorithm and artificial neural network [16]	It provides more informative features for the given dataset It supports multi objective function	Expensive is an issue	The results achieved, 93.27% accuracy, indicate the capability of the butterfly optimization algorithm to determine discriminative features of network traffic data
5	Local-Global best Bat Algorithm for Neural Networks (LGBA-NN) [17]	It is fast and appropriate for the given IoT devices	It has issue with misclassification error rate	The experimental results revealed the superiority of LGBA-NN with 90% accuracy over other variants, i.e., BA-NN (85.5% accuracy) and PSO-NN (85.2% accuracy) in multi-class botnet attack detection
6	Artificial Bee Colony (ABC) [18]	It has a better performance Also, it handles network security datasets in better way	Sometimes it has issue with high dimensional dataset	It provides 84% reliability
7	Genetic Algorithm (GA) and Deep Belief Network (DBN) [19]	It selects important and relevant features from the NSL-KDD dataset GA-DBN can effectively improve the recognition rate of intrusion attacks and reduce the complexity of the	Still it has issue with f-measure metric	This method provides 89% accuracy for the given dataset

		neural network structure		
8	GC-SVM and CBC-CSOA) [20]	It provides higher accuracy, selecting the best optimal features, and the lower computational time This method produced accurate outputs this approach may be used to forecast and identify malware in IoT-based systems	However it has issue with global optimal features	CBC-CSOA algorithm gives 86% precision and 79% recall metrics

2.3 Review on classification methods for attack detection in IoT

In [21], Alqahtani et al (2020) suggested efficient and effective IoT botnet attack detection approach. The approach relies on a Fisher-score-based feature selection method along with a genetic-based extreme gradient boosting (GXGBoost) model in order to determine the most relevant features and to detect IoT botnet attacks. The Fisher score is a representative filter-based feature selection method used to determine significant features and discard irrelevant features through the minimization of intra-class distance and the maximization of inter-class distance. On the other hand, GXGBoost is an optimal and effective model, used to classify the IoT botnet attacks. Several experiments were conducted on a public botnet dataset of IoT devices. The evaluation results obtained using holdout and 10-fold cross-validation techniques showed that the approach had a high detection rate using only three out of the 115 data traffic features and improved the overall performance of the IoT botnet attack detection process.

In [22], Hanif et al (2019) suggested artificial neural network based threat detection for IoT to solve the authentication issues. It used supervised learning algorithm to detect the attacks and furthermore controller discards the commands after classifying it as threat. ANN consists of input, hidden and output layers. Input layer passes the data as signal to hidden layer where these signals are computed with the assigned weights and activation functions are used to transform an input to an output signal. This technique is able to detect attacks effectively and timely decisions are taken to tackle the attacks. ANN approach achieves an average precision of 84% and less than %8 of average false positive rate in repeated 10-fold cross-validation. This reveals the robustness, precision and accuracy of approach in large and heterogeneous dataset. Approach used in this work has the potential to considerably improve the utilization of intrusion detection systems.

In [23], Banaamahet al (2022) explores intrusion detection methods implemented using deep learning, compares the performance of different deep learning methods, and identifies the best method for implementing intrusion detection in IoT. This research is conducted using deep learning models based on convolutional neural networks (CNNs), long short-term memory (LSTM), and gated recurrent units (GRUs). A standard dataset for intrusion detection in IoT is considered to evaluate the model. Finally, the empirical results are analyzed and compared with the existing approaches for intrusion detection in IoT. The method seemed to have the highest accuracy compared to the existing methods.

In [24], Roy et al (2018) presented a novel deep learning technique for detecting attacks within the IoT network using Bi-directional Long Short-Term Memory Recurrent Neural Network (BLSTM RNN). A multi-layer Deep Learning Neural Network is trained using a novel benchmark data set: UNSWNB15. This paper focuses on the binary classification of normal and attack patterns on the IoT network. The experimental outcomes show the efficiency of the model with regard to precision, recall, f-1 score and FAR. The BLSTM model achieves over

95% accuracy in attack detection. The experimental outcome shows that BLSTM RNN is highly efficient for building high accuracy intrusion detection model and offers a novel research methodology.

In [25], Diro et al (2018) aimed at adopting a new approach, deep learning, to cybersecurity to enable the detection of attacks in social IoT. Cybersecurity continues to be a serious issue for any sector in the cyberspace as the number of security breaches is increasing from time to time. It is known that thousands of zero-day attacks are continuously emerging because of the addition of various protocols mainly from IoT. Most of these attacks are small variants of previously known cyber-attacks. This indicates that even advanced mechanisms such as traditional machine learning systems face difficulty of detecting these small mutants of attacks over time. The performance of the deep model is compared against traditional machine learning approach, and distributed attack detection is evaluated against the centralized detection system. The experiments have shown that our distributed attack detection system is superior to centralized detection systems using deep learning model. It has also been demonstrated that the deep model is more effective in attack detection than its shallow counter parts.

In [26], Latif et al (2020) suggested different cybersecurity attacks such as denial of service (DoS), malicious operation, malicious control, data type probing, spying, scan, and wrong setup are predicted by applying machine learning techniques. To predict the aforementioned attacks, a novel lightweight random neural network (RaNN)-based prediction model has been used in this work. To investigate the performance of the RaNN-based prediction model, several evaluation parameters such as accuracy, precision, recall, and F1 score were calculated and compared with the traditional artificial neural network (ANN), support vector machine (SVM) and decision tree (DT).

In [27], Reddy et al (2020) discussed the attack detection model for IoT using Software-defined network (SDN). The SDN controller can analyze the traffic flow, detect the anomaly, and block incoming traffic as well as the source nodes. In the SDN, a Fuzzy neural network (FNN) based attack detection system is considered which can detect attacks such as man-in-the-middle, distributed denial of service, side-channel, and malicious code. The FNN is trained and tested using NSL-KDD datasets. The evaluated performance exhibits that the FNN based attack detection system can detect the mentioned attack with an accuracy of 83%.

In [28],Farhinet al (2021) presented novel deep learning-based framework with a dense random neural network approach for distinguishing and classifying anomaly from normal behaviors based on the type of attack in the IoT. Machine learning algorithms have the improbability to explore the performance, compared with deep learning models. Distinctively, the examination of deep learning neural network architectures achieved enhanced computation performance and deliver desired results for categorical attacks. This work focuses on the complete study of experimentation performance and evaluations on deep learning neural network architecture for the recognition of seven categorical attacks found in the Distributed Smart Space Orchestration System traffic traces data set. The empirical results of the simulation model report that deep neural network architecture performs well through noticeable improvement in most of the categorical attack.

In [29], Balaji, S., and S. Sankara Narayanan (2022) offered Dynamic Distributed—Generative Adversarial Network (DD-GAN) with Improved Firefly Optimization- Hybrid Deep Learning based Convolutional Neural Network -Adaptive Neuro-Fuzzy Inference System (IFFO-HDLCNN + ANFIS) that takes gain of IoT's power, offers enhanced behavior for efficiently examining the entire traffic which traverses in the IoT. Initially, Synthetic Minority Over-Sampling Technique (SMOTE) is engaged for pre-processing of data and then Modified Principal Component Analysis (MPCA) is being applied for feature reduction. The optimal features are selected through the Improve Firefly Optimization (IFFO) for optimum fitness value to enhance the classification accuracy of HDLCNN. Finally, the intrusion detection is carried out by HDLCNN + ANFIS model, which is competent in detecting threats. The experimental results have proven that model demonstrates ability to perceive any kind of probable intrusion and anomalous behavior. In comparison to existing methods, the suggested IFFO-HDLCNN + ANFIS algorithm delivers improved intrusion detection performance regarding higher accuracy, precision, recall, f-measure, reduced False Positive Rate (FPR).

In [30], Taher et al (2022) presented novel Tunicate Swarm Algorithm (TSA) that combines a long-short-term memory-recurrent neural network. The presented model accomplishes this goal by first undergoing data pre-processing to transform the input data into a usable format. Additionally, attacks in the IoT ecosystem can be

identified using a model built on long-short-term memory recurrent neural networks. There is a strong correlation between the number of parameters and the model's capability and complexity in ANN models. It is critical to keep track of the number of parameters in each model layer to avoid over- or under-fitting. One way to prevent this from happening is to modify the number of layers in your data structure. The tunicate swarm algorithm is used to fine-tune the hyper-parameter values in the Long Short-Term Memory-Recurrent Neural Network model to improve how well it can find things. TSA is used to solve several problems that couldn't be solved with traditional optimization methods. It also improved performance and shortened the time it took for the algorithm to converge. A series of tests were done on benchmark datasets. Compared to related models, the TSA-LSTMRNN model achieved greater accuracy, recall, and precision, respectively, which indicate the superiority of the model. Refer Table 3.

Table 3. Inference of Exiting Classification Method for Attack Detection in IoT.

S.No	Methods	Merits	Demerits	Parameters improved
1	Genetic-based extreme gradient boosting (GXGBoost) model [21]	This method had a high detection rate using only three out of the 115 data traffic features and improved the overall performance of the IoT botnet attack detection process	It has issue with long training time	Genetic-based extreme gradient boosting (GXGBoost) model provides 99.96% accuracy
2	ANN method [22]	It improves the performance of the classification It has the potential to considerably improve the utilization of intrusion detection systems	In few cases, some important information is missing Hence accuracy is reduced significantly	ANN approach achieves an average precision of 84% and less than %8 of average false positive rate in repeated 10- fold cross-validation.
3	Deep learning algorithm [23]	This algorithm improves both the stability and the accuracy	In few cases, it leads computational complexity	The accuracy achieves 99.7% and precision achieve 99.6%, recall 99.9%, and F-score and detection rate 99.8%
4	BLSTM RNN method [24]	BLSTM RNN is highly efficient for building high accuracy intrusion detection model and offers a novel research methodology Lower expensive	But it has issue with precision and recall metrics	BLSTM model achieves over 95% accuracy in attack detection.
5	Novel deep learning [25]	It is computationally fast The deep model is more effective in attack detection than its shallow counter parts	However it has problem with lower accuracy values	The false alarm rate of the deep model, 0.85% is much less than that of machine learning model (6.57%).

6	RaNN -based prediction model [26]	It selects important and relevant features from the intrusion dataset It provides greater performance in terms of accuracy, precision, recall metrics	Still it has issue with f-measure metric	The results show that the proposed RaNN model achieves an accuracy of 99.20% for a learning rate of 0.01, with a prediction time of 34.51 milliseconds.
7	SDN- FNN [27]	It takes minimum time for execution The FNN based attack detection system can detect the mentioned attack with an accuracy of 83%	It has issue with expensive	It provides 83.4% as accuracy
8	Random Neural Network (RNN) approach [28]	It has a better classification performance compared with other algorithms It reported that deep neural network architecture performs well through noticeable improvement in most of the categorical attack	However it has issue with local optimal features	RNN method give 90.02% accuracy
9	DD-GAN- IFFO-HDLCNN + ANFIS [29]	This model demonstrates ability to perceive any kind of probable intrusion and anomalous behavior It provides better accuracy, precision, recall, f-measure, reduced False Positive Rate (FPR)	But it is hard to distinguish which feature should be first selected when multiple features achieve the same frequency.	DD-GAN- IFFO-HDLCNN + ANFIS provides 94.52% accuracy
10	Novel tunicate swarm algorithm that combines a long-short-term memory-recurrent neural network (TSA- LSTMRNN) [30]	It gives greater accuracy, recall, and precision metrics	It has still issue with exploration and exploitation phase.	This method provides 98.1% accuracy

3. Analysis Report

The TSA-LSTMRNN model's performance is tested usingthe KDD Cup99 Dataset [31], which contains data in fivecategories: DoS, R2L, normal, U2R, and Probe.Many studies have used theKDDCup99 dataset to

evaluatethe performance of IDS. Even though the dataset is outdated,it is still helpful to examine the IDS models. Because thesame dataset yields a plethora of performance measurement findings. We choose the KDD Cup99 dataset primarily forthis reason.The dataset contains 4,898,431 network traffics, each with41 unique attributes. In addition, there are 22 distinct typesof attacks. Table 1 categorizes the assaults. When a DoSattack is launched, the target servers' resources are depleted,preventing any service from being provided. It is possible togain remote access to a computer without authorization whenusing an R2L attack. An attack known as U2R aims to gaincontrol of the system's superuser privileges. The purpose of a probing attack is to determine whether the targeted server is vulnerable.

For the experiments, MATLAB is used to evaluate the existing classification models and comparisons. SDN-FNN, RNN, HDLCNN+ANFIS and TSA-LSTMRNN algorithms are evaluated in terms of accuracy, precision, recall and f-measure metrics. Table 4 represents the category of the attacks and Table 5 represents the performance analysis.

Table 4. Category of the Attacks.

Category	**Attacks**
DoS	Back, land, Neptune, pod, smurf, teardrop
R2L	ftp- write, quess-passwd, imap, multihop, phf, spy, warezelient, warezmaster
U2R	Buffer-overflow, loadmodule, perl, rootkit
Probe	Ipsweep, nmap, portsweep, satan

Table 5. Performance Comparison

Methods	**KDD Cup99 dataset**			
	Accuracy	**Precision**	**Recall**	**F-measure**
SDN-FNN	83.4	75.45	78.96	77.2
RNN	90.02	80.56	84.22	82.39
HDLCNN+ANFIS	94.52	82.61	87.12	84.86
TSA-LSTMRNN	98.1	85.59	92.34	88.96

1. Accuracy

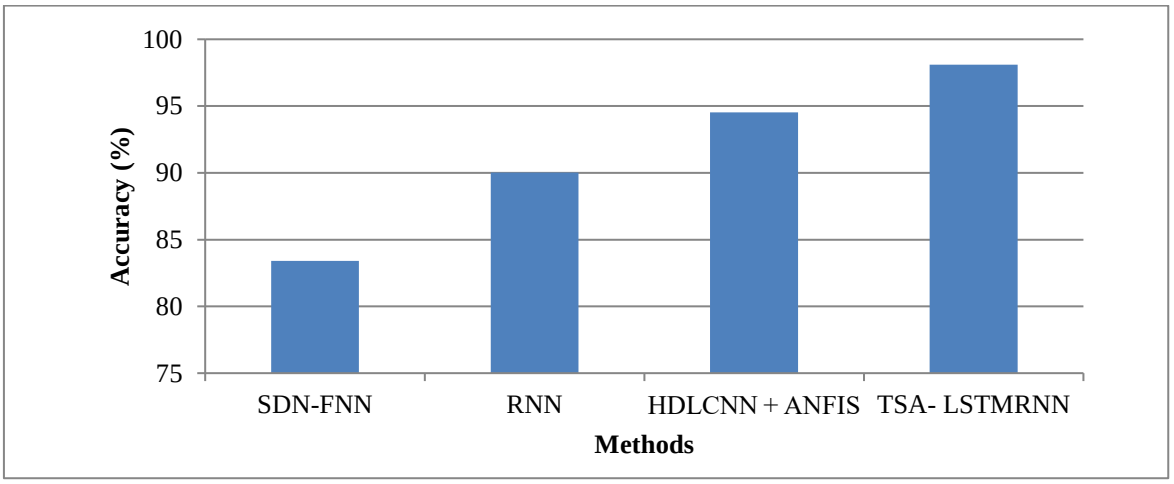
Accuracy is the most intuitive performance measure and it is simply a ratio of correctly predicted observation to the total observations.

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+FN+TN} \quad (1)$$

Where,

TP - True Positive, FN - False Negative, FP - False Positive, TN- True Negative

Figure 1.*Accuracy*



From the above Figure1, it can be observed that the comparison metric is evaluated using existing methods in terms of accuracy. For x-axis the methods are taken and in y-axis the accuracy value is plotted. The TSA-LSTMRNN algorithm provides higher accuracy while the other existing SDN-FNN, RNN and HDLCNN+ANFIS algorithms provide lower accuracy values for the given KDD Cup99 dataset. Thus the result concludes that the TSA-LSTMRNN algorithm increase the attack detection accuracy over the IoT environment.

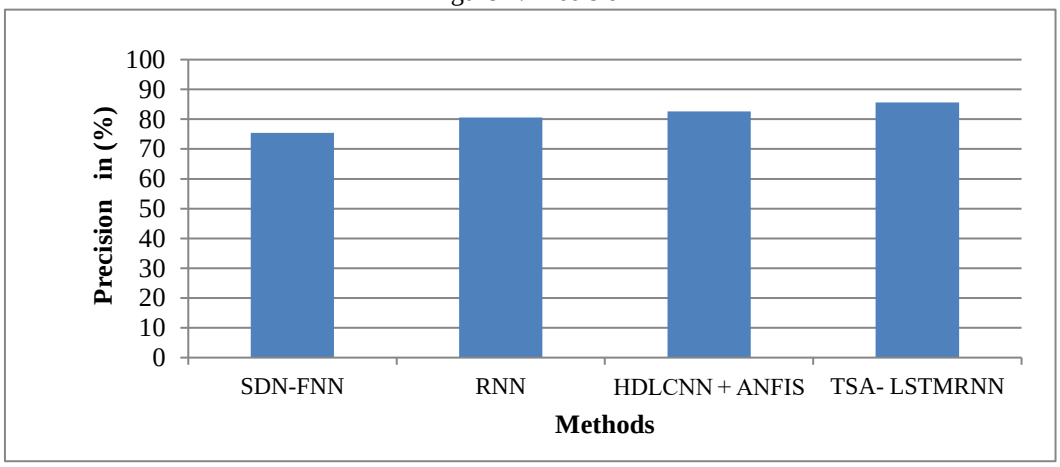
2. Precision

Precision is the ratio of correctly predicted positive observations to the total predicted positive observations.

$$\text{Precision} = \frac{TP}{TP+FP} \quad (2)$$

Where, TP - True Positive, FP - False Positive

Figure 2. *Precision*



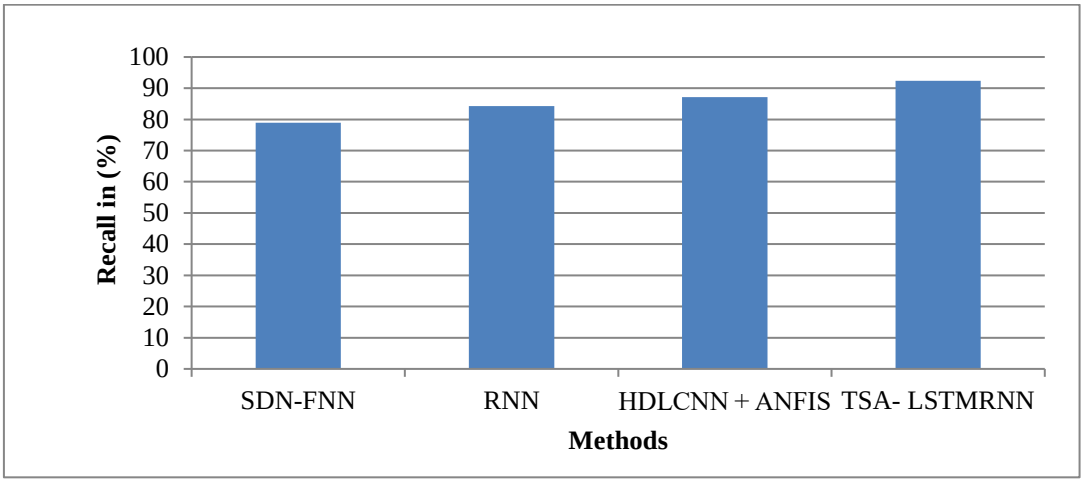
From the above Figure2, it can be observed that the comparison metric is evaluated using existing methods in terms of precision. For x-axis the methods are taken and in y-axis the precision value is plotted. The TSA-LSTMRNN algorithm provides higher precision while the other existing SDN-FNN, RNN and HDLCNN+ANFIS algorithms provide lower precision values for the given KDD Cup99 dataset. Thus the result concludes that the TSA-LSTMRNN algorithm increase the attack detection accuracy over the IoT environment.

3. Recall

Recall is the ratio of correctly predicted positive observations to the all observations in actual class.

$$\text{Recall} = \frac{TP}{TP+FN} \quad (3)$$

Figure 3. Recall



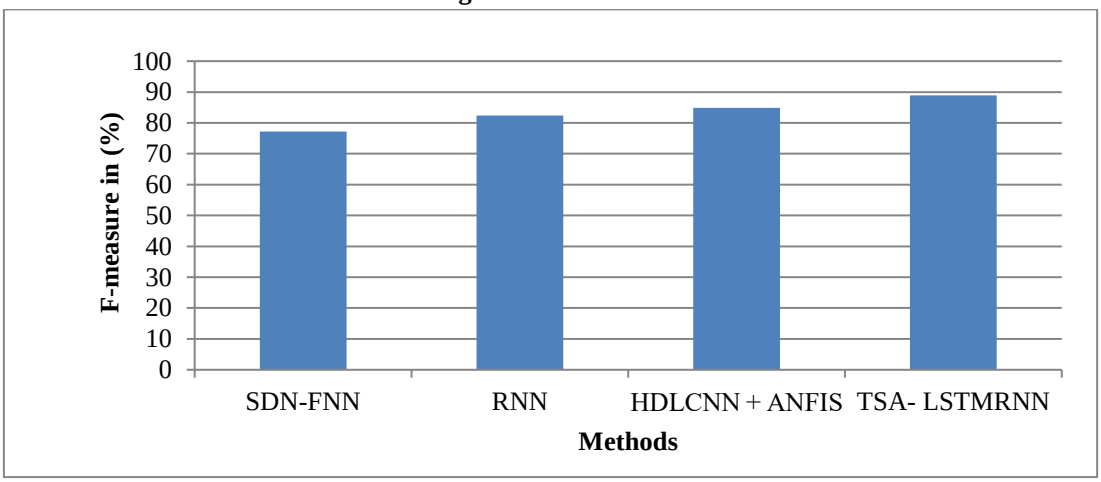
From the above Figure3, it can be observed that the comparison metric is evaluated using existing methods in terms of recall. For x-axis the methods are taken and in y-axis the recall value is plotted. The TSA-LSTMRNN algorithm provides higher recall while the other existing SDN-FNN, RNN and HDLCNN+ANFIS algorithms provide lower recall values for the given KDD Cup99 dataset. Thus the result concludes that the TSA-LSTMRNN algorithm increase the attack detection accuracy over the IoT environment.

4. F-measure

F1 Score is the weighted average of Precision and Recall. Therefore, this score takes both false positives and false negatives into account.

$$\text{F-measure} = 2*\frac{(\text{Recall}*\text{Precision})}{(\text{Recall}+\text{Precision})} \quad (4)$$

Figure 4. F-measure



From the above Figure 4, it can be observed that the comparison metric is evaluated using existing methods in terms of F-measure. For x-axis the methods are taken and in y-axis the F-measure value is plotted. The TSA-LSTMRNN algorithm provides higher F-measure while the other existing SDN-FNN, RNN and HDLCNN+ANFIS algorithms provide lower F-measure values for the given KDD Cup99 dataset. Thus the

result concludes that the TSA-LSTMRNN algorithm increase the attack detection accuracy over the IoTEnvironment.

4. Conclusion

This survey discussed the attack detection in IoT environment using the existing methods. Various methods are analyzed on the given KDD cup99 dataset to improve the attack detection performance. As a result, the data preprocessing performed by the presented model is used to convert the input data into a format that can be used. In addition, the classification model is used for the identification and classification of attacks in the IoT environment. It also analyzed the advantages and shortcomings of each technique applied to theattack detection in IoT. So it can say that this survey will provide a beneficial glance of existing solution with their implementation, advantages and shortcomings. However, the existing algorithms have issue with recognizing the strengths and weaknesses of their attack findings. To overcome this issue, TSA-LSTMRNN approach is introduced for the better attack detection accuracy and The TSA is used to properly adjust the hyper-parameter values involved in the LSTMRNN model to improve the detection outcomes of the model. However, in this survey, optimized feature selection is still not achieved effectively on the given IoT systems. In future work, ensemble optimization based algorithms can be developed for improving the various attack detection performance.

5. References

[1] A. K. Sahu, S. Sharma, M. Tanveer, and R. Raja, "Internet of Things attack detection using hybrid Deep Learning Model," *Computer Communication*, vol.176,pp.146-154, 2021.

[2] K. N. Qureshi, S. S. Rana, A. Ahmed, and G. Jeon, "A novel and secure attacks detection framework for smart cities industrial internet of things," *Sustainable Cities and Society*, vol.61,pp.102343, 2020.

[3] A. Mihoub, O.B. Fredj, O. Cheikhrouhou, A. Derhab, and M. Krichen, "Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques," *Computers & Electrical Engineering*, Eng, vol. 98,pp. 107716, 2022.

[4] W. B Daoud, and S. Mahfoudhi, "SIMAD: Secure Intelligent Method for IoT-Fog Environments Attacks Detection," *Computers Material & Continua*, vol. 70, no.2, 2022.

[5] M. A. Ambusaidi, X. He, Z. Tan, P. Nanda, L. F. Lu, and U. T. Nagar, "A novel feature selection approach for intrusion detection data classification," *13th international conference on trust, security and privacy in computing and communications*, IEEE, 2014.

[6] M. Anwer, S. M. Khan, and M. U. Farooq, "Attack detection in IoT using machine learning," *Engineering, Applied Science Research*, vol.11, no.3, pp. 7273-7278, 2021.

[7] R. Pecori, A. Tayebi, A. Vannucci, and L. Veltri, "IoT Attack detection with deep learning analysis," *International Joint Conference on Neural Networks (IJCNN)*, IEEE, 2020.

[8] G.K. Baydoğmuş, "The Effects of Normalization and Standardization an Internet of Things Attack Detection," *AvrupaBilimveTeknolojiDergisi*, vol.29,pp. 187-192, 2021.

[9] M. G. Karthik, and M.M. Krishnan, "Hybrid random forest and synthetic minority over sampling technique for detecting internet of things attacks," J. *Journal of Ambient Intelligence and Humanized Computing*, pp.1-11, 2021.

[10] M.S.A. Muthanna, R. Alkanhel, A. Muthanna, A. Rafiq, and W.A.M. Abdullah, "Towards SDN-enabled, intelligent intrusion detection system for internet of things (IoT)," *IEEE Access*, vol. 10, pp. 22756-22768, 2022.

[11] S. Roy, J. Li, B.J. Choi, and Y. Bai, "A lightweight supervised intrusion detection mechanism for IoT networks," *Future Generation Computer System*, vol.127, pp. 276-285, 2022.

[12] D. K. K. Reddy, H. S. Behera, J.Nayak, B. Naik, U. Ghosh, and P. K. Sharma,"Exact greedy algorithm based split finding approach for intrusion detection in fog-enabled IoT environment," J. *Journal of Information Security and Applications*, vol. *60*, 2021.

[13] P. K. Keserwani, M.C. Govil, E.S. Pilli, and P. Govil, "A smart anomaly-based intrusion detection system for the Internet of Things (IoT) network using GWO–PSO–RF model," *Journal of Reliable Intelligent Environments* , vol. 7, pp. 3-21, 2021.

[14] J. Liu, D. Yang, M. Lian, and M. Li, "Research on intrusion detection based on particle swarm optimization in IoT," *IEEE Access*, vol. 9, pp.38254-38268, 2021.

[15] E.P. Krishna, and A. Thangavelu,"Attack detection in IoT devices using hybrid metaheuristic lion optimization algorithm and firefly optimization algorithm", *InternationalJournal of Systems Assurance*, pp.1-14, 2021.

[16] Y. Li, S.M.Ghoreishi, and A. Issakhov, "Improving the accuracy of network intrusion detection system in medical IoT systems through butterfly optimization algorithm," *Wireless Personal Communications*, vol. 126, no. 3, pp. 1999-2017, 2022.

[17] A. Alharbi, W. Alosaimi, H. Alyami, H. T. Rauf, and R. Damaševičius, "Botnet attack detection using local global best bat algorithm for industrial internet of things," *Electronics*, vol.10, no. 11 2021.

[18] M. Stankovic, M. Antonijevic, N. Bacanin, M. Zivkovic, M. Tanaskovic, and D. Jovanovic, "Feature selection by hybrid artificial bee colony algorithm for intrusion detection," *International Conference on Edge Computing and Applications (ICECAA)*. *IEEE*, 2022.

[19] Y. Zhang,P. Li, and X. Wang, "Intrusion detection for IoT based on improved genetic algorithm and deep belief network," *IEEE Access*, vol. 7, pp. 31711-31722, 2019.

[20] S. K. Gupta, B. Pattnaik, V. Agrawal, R.S.K. Boddu, A. Srivastava, and B. Hazela,"Malware Detection Using Genetic Cascaded Support Vector Machine Classifier in Internet of Things," *Second International Conference on Computer Science, Engineering and Applications (ICCSEA)*. *IEEE, 2022.*

[21] M. Alqahtani, H. Mathkour, and M.M. Ben Ismail, "IoT botnet attack detection based on optimized extreme gradient boosting and feature selection," *Sensors*, vol.20, no.21,2020.

[22] S. Hanif, T. Ilyas, and M. Zeeshan. "Intrusion detection in IoT using artificial neural networks on UNSW-15 dataset," *IEEE 16th international conference on smart cities: improving quality of life using ICT &IoT and AI (HONET-ICT)*. IEEE, 2019.

[23] A. M. Banaamah, and I. Ahmad, "Intrusion Detection in IoT Using Deep Learning," *Sensors*, vol. 22, no. 21, pp. 8417, 2022.

[24] B. Roy, and H. Cheung, "A deep learning approach for intrusion detection in internet of things using bi-directional long short-term memory recurrent neural network." 2018 *28th international telecommunication networks and applications conference (ITNAC)*.IEEE, 2018.

[25] A.A. Diro, and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Future Generation Computer System*, vol. 82, pp. 761-768, 2018.

[26] S. Latif, Z. Zou, Z. Idrees, and J. Ahmad, "A novel attack detection scheme for the industrial internet of things using a lightweight random neural network," *IEEE access* vol. 8,pp. 89337-89350,2020.

[27] D. K. Reddy, H. S. Behera, J. Nayak, P. Vijayakumar, B. Naik, and P. K. Singh, "Deep neural network based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities," *Emerging Telecommunications Technologies*, vol. 32, no. 7, 2021.

[28] F. Farhin, I. Sultana, N. Islam, M.S. Kaiser, M.S. Rahman, and M. Mahmud, "Attack detection in internet of things using software defined network and fuzzy neural network," *2020 Joint 9th International Conference on Informatics, Electronics & Vision (ICIEV) and 2020 4th International Conference on Imaging, Vision & Pattern Recognition (ICIVPR)*. IEEE, 2020.

[29] S. Balaji, and S. S. Narayanan, "Dynamic distributed generative adversarial network for intrusion detection system over internet of things," *Wireless Networks*, 1-19, 2022.

[30] F. Taher, M. Elhoseny, M. K. Hassan, and I. M. El-Hasnony, "A Novel Tunicate Swarm Algorithm with Hybrid Deep Learning Enabled Attack Detection for Secure IoT Environment," *IEEE Access*, vol. 10, pp.127192-127204, 2022.

[31] Cup, K. D. D. "http://kdd. ics. uci. edu/databases/kddcup99/kddcup99. html." The UCI KDD Archive 1999.

[32] Ms.U.Sinthuja&Dr.S.Thavamani, 2019. "Analyzing DOS Attacks In Publish Subscribe IOT Networks" in *International Journal of Exclusive Management Research* (IJEMR) (www.ijemr.in), Volume 9, August Special Issue 2019, Page No. 130-133, Impact Factor – 5.76, Print : ISSN 2249 -8672.

[33] Ms.U.Sinthuja&Dr.S.Thavamani, 2019. "Efficient Employment of the MQTT and S-MQTT Protocol in IOT Network" in the *International Journal of Advanced Science and Technology*, Vol.28, No.17, 2019, PP: 858-864, ISSN : 2005-4238 IJAST. ELSEVIER Indexed bySCOPUS (http://sersc.org/journals/index.php/IJAST/article/view/2448

[34] Ms.U.Sinthuja&Dr.S.Thavamani, 2019. "Evaluating Systems And Tools For Vulnerability Study On Multi-Broker MQTT Instances " *National Journal of GEDRAG & ORGANISATIE REVIEW Web of Science Group with Care UGC Gruop – II*, Vol.33, Issue.4, PP : 607-615, ISSN : 0921-5077, Nov 2020 (http://lemma-tijdschriften.com/)

[35] Ms.U.Sinthuja&Dr.S.Thavamani, 2021. "MQTT Messages An Overview "*International Journal of Mathematics and Computer Research*, Vol.9, Issue.4, PP : 2267 - 2270, ISSN : 2320-7167, April 2021, Index Copernicus ICV: 57.55, Impact Factor: 7.184 http://ijmcr.in/index.php/ijmcr/article/view/311/283.

[36] Ms.U.Sinthuja&Dr.S.Thavamani, 2021. "The MQTTset Training and Varients of Denial of Service Prediction Using The LSTMQ Model "*Journal of Stochastic Modeling& Applications*, ISSN No : 0972-3641, Page No : 1-4. Volume No : 28 , Issue No : 6, Special Issue 2022 Part 13, Jan-June 2023, *UGC Care Approved Journal UGC CareApproved Journal*.