Annals of Emerging Technologies in Computing (AETiC)
Vol. 4, No. 5, 2020

Research Article

A Novel Hybrid Intrusion Detection System (IDS) for the Detection of Internet of Things (IoT) Network Attacks

Rabie A. Ramadan[1,2,*] and Kusum Yadav[1]

[1]Computer Science and Engineering College, University of Hai'l, Hai'l, Saudi Arabia
rabie@rabieramadan.org

[2]Computer Engineering Department, Cairo University, Giza, Egypt
y.kusum@uoh.edu.sa

*Correspondence: rabie@rabieramadan.org

Received: 8th November 2020; Accepted: 11th December 2020; Published: 20th December 2020

Abstract: Nowadays, IoT has been widely used in different applications to improve the quality of life. However, the IoT becomes increasingly an ideal target for unauthorized attacks due to its large number of objects, openness, and distributed nature. Therefore, to maintain the security of IoT systems, there is a need for an efficient Intrusion Detection System (IDS). IDS implements detectors that continuously monitor the network traffic. There are various IDs methods proposed in the literature for IoT security. However, the existing methods had the disadvantages in terms of detection accuracy and time overhead. To enhance the IDS detection accuracy and reduces the required time, this paper proposes a hybrid IDS system where a pre-processing phase is utilized to reduce the required time and feature selection as well as the classification is done in a separate stage. The feature selection process is done by using the Enhanced Shuffled Frog Leaping (ESFL) algorithm and the selected features are classified using Light Convolutional Neural Network with Gated Recurrent Neural Network (LCNN-GRNN) algorithm. This two-stage method is compared to up-to-date methods used for intrusion detection and it over performs them in terms of accuracy and running time due to the light processing required by the proposed method.

Keywords: ***IoT; Hybrid classification; IoT security; Convolution Neural Network; KDD cup dataset***

1. Introduction

Internet of Things (IoT) becomes more increasingly popular in different industries such as social domains, healthcare, personal and smart cities. However, it increases the risk of security issues in many applications like medical monitoring, mission-critical tasks, and industrial control. These applications work mainly based on trustworthy data delivery, data privacy, and reliability. Due to the limitations of the IoT technologies, security became one of the key issues in IoT services and networks. The IoT devices are tiny, heterogeneous and not supporting interoperability. These characteristics extend the attack range and increase the complexity of developing any security solution. IoT devices are vulnerable to not only network attacks (Putra, Dedeoglu, Kanhere, and Jurdak, 2020)(Daia, Ramadan, and Fayek, 2018), they are also susceptible to powerful hackers from unauthorized internet users. In some of the literatures, cryptography algorithms are proposed for IoT authenticity and confidentiality to some extent. However, cryptography tools are costly in terms of computations and time which might not be suitable for IoT devices.

Rabie A. Ramadan and Kusum Yadav, "A Novel Hybrid Intrusion Detection System (IDS) for the Detection of Internet of Things (IoT) Network Attacks", *Annals of Emerging Technologies in Computing (AETiC)*, Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 61-74, Vol. 4, No. 5, 20th December 2020, Published by International Association of Educators and Researchers (IAER), DOI: 10.33166/AETiC.2020.05.004, Available: http://aetic.theiaer.org/archive/v4/v4n5/p4.html.

In addition, cryptography algorithms help in satisfying network authentication and data integrity. Additional tools are required to monitor the IoT network traffic to avoid the recent network attacks. Intrusion Detection System ((IDS) is most essential to maintain such function. IDSs play the role of network monitoring, analysis, and attack detection.

Various IDS techniques are presented in the literature. These techniques are categorized into two types which are anomaly-based detection and signature-based detection (Blanco, Malagón, Briongos, and Moya, 2019) [4]. The signature-based detection method depends on the history of pre-defined malicious activities patterns and the anomaly-based detection method depends on the discovery of the deviation from normal behaviors to determine the intrusions. Therefore, the anomaly-based method had the capability of detecting unknown attacks without predefined activity patterns. In this paper, we present an anomaly-based intrusion detection model in IoT networks.

One of the anomaly-based methods is clustering. Clustering techniques can determine the intrusions without predefined patterns. For instance, the authors of (Jyothsna, V. Rama Prasad, and Munivara Prasad, 2011) experimented with k-means, k-medoids, outlier detection algorithms and EM clustering to detect network intrusions. Through clustering, the traffic could be divided into normal and abnormal traffic [6]. However, EM-based anomaly detection method turns out to provide more accurate results than other clustering methods. Other classification methods are utilized for anomaly detection such as Fuzzy logic, classification tree, Naïve Bayes network, genetic algorithm, Support vector machine, and neural network [7]. The main idea behind the operation of these algorithms is to classify the data into two types such as normal or abnormal categories. When multiple numbers of attacks presented in-network, single algorithm might not be sufficient. Hybrid approaches are used to use cascaded supervised algorithms, cascaded unsupervised algorithms, or combining supervised and unsupervised algorithms [8] [9].

The research in this paper falls under the umbrella of the hybrid approach where the main objectives are:

- To select more relevant features using Enhanced Shuffled Frog Leaping (ESFL) algorithm,
- To achieve the high classification rate using Light Convolutional Neural Network with Gated Recurrent Neural Network (LCNN-GRNN) method,
- To improve the detection rate accuracy of certain attacks such as U2R, DoS, R2L attacks without mitigating of performance. Those attacks are the most attacks recently discovered for IoT networks.

The paper is organized as follows: Section II defines the various literature survey of IDS techniques and IoT security challenges. Section II defines the problem to be solved in this paper. Section IV describes the overall workflow of the proposed system and a detailed description of the proposed hybrid methods and algorithms. Section V contains the performance analysis of the proposed system and dataset description. Section VI concludes the proposed system results and discussion.

2. Problem Definition

With the advances in sensing technologies, IoT network became possible. However, IoT devices suffer from different limitations including the energy sources and limited capabilities. In addition, standard cryptography and regular IDS techniques could not be suitable for such network. Besides, with the connectivity to the Internet, hacking techniques are getting strong and easy to be learnt. Therefore, efficient monitoring process for intrusion detection is a challenge. This leads to various research proposals to enhance IoT intrusion detection performance. One of the famous datasets that has been extensively studied is NSL-KDD cup dataset. It became a de facto standard to test new algorithms. Unfortunately, the existing methods suffer from the following problems:

- Minimum classification rate of attacks,
- Time overhead,
- Minimum detection rate of attack and
- Minimum accuracy.

Therefore, the problem in hand is to introduce an efficient IDS solution that solve the following mentioned problems where the detection time is important especially with IoT runtime operation. Also, the accuracy is another issue where IoT systems could be used in critical applications such as healthcare or military systems.

This paper proposes a hybrid IDS system that combines CNN and Gated Recurrent Neural Network, LCNN-GRNN. In addition, it proposes a pre-processing method entitled Enhanced Shuffled Frog Leaping (ESFL) for the best feature selection operation. To improve the performance of the proposed system, the dataset is split into training and testing sub-data before classification. It classifies the information into normal class or anomaly class.

3. Literature Review

Chaabouni *et al.* [10] classified the IoT security attacks in IoT networks using existing anomaly detection approaches. They survey the state-of-the-art NIDS - Network Intrusion Detection System describing various existing NIDS implementation tools, open-source network sniffing software, and datasets. This review comprises the existing NIDS techniques with machine learning techniques and the conclusion was that machine learning techniques give higher success rate than other techniques.

Pajouh *et al.* in [11] presented the novel IDS system based on the two-tier classification module and two-layer dimension reduction to determine the malicious activities named R2L and U2R attacks. The proposed method examined the linear discriminant analysis and component analysis of dimension reduction for feature selection or dimensionality reduction. Then, the authors applied the two-tier classification method in the form of K-NN and naïve Bayes to analyze the suspicious behaviors. The proposed method was examined with the NSL-KDD dataset and the authors claimed that the proposed method of superior performances to determine R2L and U2R attacks.

The IoT becomes much more interests in many industries such as logistics tracking, healthcare, automobile, and smart cities. Hodo *et al.* in [12] described the threat analysis in IoT and ANN algorithm was used to analyze these threats. A supervised ANN or multilevel perceptron was trained by internet packet traces, then evaluated the ability of the proposed system to DDoS attacks. The paper focuses on the classification of normal and attack patterns in IoT networks. The authors claimed that they were able to detect up to 99.4% of DDoS attacks in the used datasets.

Another work has been conducted by Deng *et al.* in [13] where they proposed an IDS system for mobile networks based on a transfer learning algorithm. the authors analyzed various security issues and characteristics of networking security. Then, they discussed the internet security technologies of authentication, key management, routing security, access control, intrusion detection, fault tolerance, and privacy protection. Also, various types of intrusion detection technologies were discussed and the applications of IoT architecture were identified.

Midi *et al.* [14] proposed a knowledge-driven adaptable IDS system (KALIS) for IoT. KALIS is designed to be able to detect intrusions across a wide range of IoT systems in real-time. The proposed system monitors numerous protocols and it had no performance impacts on IoT applications. The proposed IDS approach does not mark individual protocols for IoT networks. It familiarizes the suitable detection strategy to certain network features. The authors claimed that that KALIS algorithms is effective in detecting intrusions of IoT systems.

Similar algorithm is proposed in [15] where deep learning is utilized for traffic flow intrusion detection in IoT networks. The proposed method generates the generic features from packet-level information. The authors developed Feed Forward Neural Networks (FFNN) to detect Dos, DDOS, information theft attacks, and reconnaissance for binary and multiclass classification. Again, the authors claimed the effectiveness of their algorithm in attacks detection and classification.

Another deep leaning approach is presented in [16] where the authors proposed a new intrusion detection system named as mutual information selection element and deep extraction. The feature extraction process was done using deep structure stacked autoencoders based on mutual information between the class label and the feature. The entropy-based tree wrapper method was utilized for optimizing the feature subsets.

In [17], Zhang and his colleagues proposed an IDS system based on a hybrid approach of Deep Belief Network and Genetic algorithm. This algorithm determined various kinds of attacks over multiple iterations of GA. The NSL-KDD dataset was used for evaluation and the results showed that the presented IDS model enhances the intrusion detection rate and minimizes the neural networks structure complexities.

Near-real-time IDS system IoT networks by using Apache spark and supervised learning was proposed in [18]. In this paper, various machine learning algorithms were discussed identifying the cyber-attacks IoT system and compared these algorithms based on their performance measures. The authors selected the supervised machine learning techniques in the MLlib library of Apache spark for big data processing. From the overall techniques, the Random Forest achieved an accuracy of 1 and also showed a 23.22 second of short training time. Moreover, the explicit model was generated by RF due to its easy implementation of low-level programming languages. The proposed hybrid approach determines the SYN-DOS cyber-attacks with identification performance and computation time on IoT devices.

For specific attacks such as Sybil attack, Murali *et al.* [19] proposed an effective algorithm for multiple illegal attack activities. This research presented Artificial Bee Colony (ABC) algorithm for mobile Sybil attack. The lightweight IDS system was utilized for Sybil attack in mobile RPL. Furthermore, they considered three Sybil attack categories based on their behaviour. They determined the RPL Sybil attack based on energy consumption, traffic overhead, and PDR – Packet Delivery Ratio. They evaluated the proposed algorithm of performances based on sensitivity, specificity, and accuracy.

In [20], a decentralized collaborative intrusion detection system for IoT applications was developed. The proposed IDS system mainly uses blockchain technology. it tries to satisfy the security of the data storage elements and assure and distributed trust. The proposed architecture provides a liable trust environment that promotes penalties, incentives and scalable intrusion information storage by bloom filters.

Rules and Decision Tree-based IDS (RDTIDS) system for IoT networks is proposed in [21]. The RDTIDS system comprises the various classifier methods based on rules-based concepts and decision tree named as JRip algorithm, REP tree, and Forest PA. Similarly, PCA algorithm is used in [18] where the research introduced the ultrahigh-frequency RFID sensor system for characterization and corrosion detection. The 3-D antenna sensor was used for feature selection.

Graph theory is also used to analyze intrusions in the IoT network and a hybrid intrusion detection systems ware presented in [22]. The proposed system contains Distributed and Passive EEA (Energy Exhaustion Attack) and Centralized and Active Malicious Node Detection (CAMD). It determines the malicious nodes integrated by cybercriminals and gives the digital evidence for forensics. The algorithm was implemented to detect the influences of EEA attacks in a group of communication protocols. The evaluation results proved that the proposed hybrid IDS systems are more efficient in terms of energy than other algorithms.

A good survey on recent intrusion detection algorithms and different important tools to protect the network and information systems were presented in [23]. It shows that the traditional IDS methods are difficult to apply on IoT networks due to its special characteristics in terms of the used protocol stacks, constrained resource devices, and standards.

The main objective of this research is to analyze the IoT open security issues and proposes an IDS that is more accurate and time efficient.

4. Proposed IDS System

This section provides a detailed description of the proposed IDS system to detect the intrusions in IoT networks. Different steps are involved in the proposed hybrid IDS system. Due to the huge data collected from IoT networks, it is proposed in this paper to have a pre-processing stage. The data pre-processing is attained by data normalization and dimensionality reduction. The relevant features are extracted using Enhanced Shuffled Frog Leaping (ESFL) algorithm. Then, the extracted relevant features are used in the classification of the traffic data. After feature selection, the relevant features

are attained for training and testing. The classification process is done by using hybrid IDS system named Light Convolutional Neural Network with Gated Recurrent Neural Network (LCNN-GRNN).

This classification determines whether the information presents in a normal class or anomaly class. The proposed hybrid model tuned some important parameters like several estimators to achieve better accuracy. The overall proposed IDS system is described in figure 1.

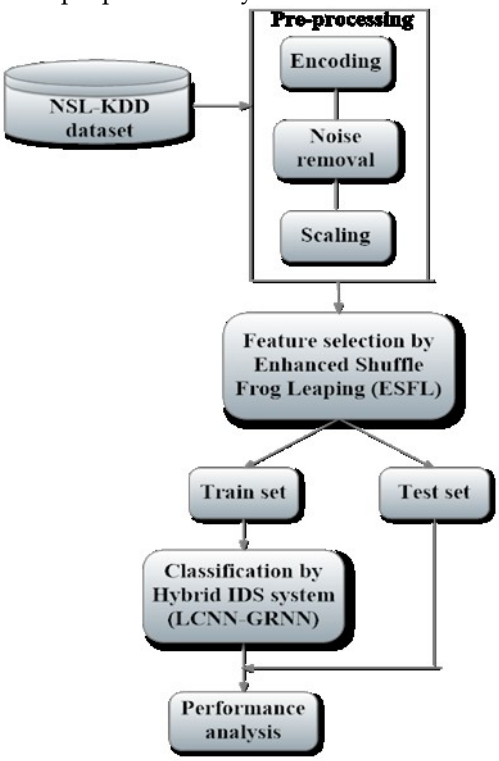

Figure 1. The proposed flow of the overall system

As can be seen in the figure, the input of the system is the dataset such as NLS-KDD, this dataset is feed into the pre-processing phase where the data is encoded following by noise removal process and scaling. The scaled data is used as an input to the Enhanced Shuffled Frog Leaping (ESFL)for feature selection. Consequently, the selected features are divided into training and testing subsets. At this stage, LCNN-GENN came to place where the classification is made. The final stage is the proposed algorithm performance measure.

4.1. Pre-processing

Looking at the most of the datasets used in the literature, it has been found that they contain noise, insignificant features, missing values and redundant data that leads to inefficient and inaccurate classification results. Also, the processing time is increased when the overall features are used. The pre-processing phase helps to eliminate incomplete and redundant data and to transform the data into a uniform format which means it converts the raw dataset into a clean dataset before feeding it into the proposed algorithm. The effective pre-processing method is required to improve the raw data quality without any information loss.

The proposed pre-processing process performs the following steps, see Figure 1:

1. Encoding
2. Noise removal
3. Scaling

The initial dataset contains multiple labels in numerous columns. The labels are defined in the form of numbers or words. Encoding refers to transforming the labels into numeric form, it's called as converting of human-readable format into a machine-readable format. The noise removal process removes the irrelevant features of noises by using filters. The scaling method scales the large amount

of numerical data based on the features of distance values. By using these methods, the pre-processed features are involved in the feature selection process.

4.2. Feature Selection

The pre-processed features are attained to feature selection by Enhanced Shuffled Frog Leaping (ESFL) algorithm. This population-based algorithm works mainly based on random search and probability. In this algorithm, the features selection inspired by frogs' and detecting foods in wetlands. It works as an optimization problem where the positions with the highest fitness is the one with more food. The initial population of frogs is randomly dispersed in search space like other feature optimization methods.

In the proposed ESFL algorithm, the individuals are allotted to multiple groups and the worst individual(Q_x^t) has learned from the subgroup of the best individual(Q_c^t). When no progress is learned from a global best individual, then, no progress will be replaced by a random individual.

$$\text{Len}^t = S \times (Q_c^t - Q_x^t) \quad (1)$$

In multiple numbers of iterations (t), the new individual is generated by,

$$Q_x^{t+1} = Q_x^t + \text{Len}^t \quad (Len_k \geq \text{Len} \geq -Len_k) \quad (2)$$

Where: $Q_x^{t+1} = (Q_{x1}^{t+1}, Q_{x2}^{t+1} \ldots\ldots Q_{xn}^{t+1})$

Here, Q defines a random number in the range [0,……1], $-Len_k$ and Len_k define the range of leaping step values. If newly generated Q_x^{t+1} is an improvement over old Q_x^t, it will replace by a new individual.

4.2.1. Memory Weight Calculation

The balance between local search ability and global exploration was controlled by memory weight in which it increases the search ability. To improve the proposed system performance, the memory weight was used by the logistic map.

In several "t" iterations, the memory weight is calculated by,

$$\text{Len}^{t+1} = X(t+1) \times \text{Len}^t + s \times (Q_c^t - Q_x^t)$$

$$x(t+1) = 4.0 \times x(t) \times (1 - x(t)) \quad (Len_k \geq \text{Len} \geq -Len_k) \quad (3)$$

Sorting of individuals

In the ESFL algorithm, the individuals are sorted and allotted to each group based on the fitness values. The best individuals are assigned to the first group and worst individuals are assigned to the last group. When the individuals are limited in the first group, the algorithm determines that it is difficult to leave from the local optimum. In each group, it is required to balance the individual's fitness with the balancing number of each group.

Representation of feature subset:

Finally, the basic Shuffled Frog Leaping method should be convert Q_x into a binary form. Q_x is transformed into a binary range [0, 1] by,

$$\text{sig(Len)} = \frac{1}{1+e^{-B*Len}} \quad (4)$$

$$B = = \frac{h}{H}(\text{factor1} - \text{factor 2}) + \text{factor2} \quad (5)$$

$$\text{new}Q_x = \begin{cases} 1 \text{ if } (\text{sig(Len)} > S) \\ 0 \text{ if } (\text{sig(Len)} \leq S) \end{cases} \quad (6)$$

In number of selected features, the fitness function is calculated by,

$$\text{fitness} = x_1 \times \text{acc (Jnn)} + x_2 \times (1 - \frac{n}{N}) \quad (7)$$

x_1 and x_2 are the selected features and the accuracy defines the relationship among the number of selected features and the number of overall features.

$$\text{acc} = \frac{num_a}{num_a + num_i} \times 100 \quad (8)$$

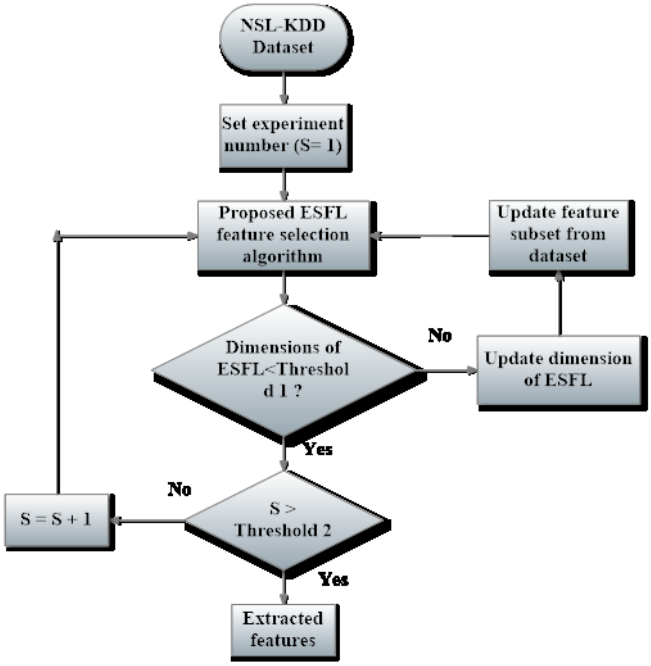

Figure 2. Flowchart of the proposed feature selection algorithm

Figure 2 represents the flow chart of the proposed feature selection (ESFL) method and Algorithm1 shows its details.

Algorithm 1. Enhanced Shuffled Frog Leaping (ESFL)

- Step 1: Randomly generate a population of F=k×n individuals. Where (k) represents the number of subgroups, (n) represents the number of individuals in each subgroup, and each individual is converted to a binary number set by equations (4) and (5).
- Step 2: Use the evaluation function to calculate the value for each individual and identify the global best individual (Q_x).
- Step 3: Then soring of individuals sort (F) into descending order and assign them to (k) subgroups where each subgroup contains (n) individuals.
- Step 4: Find the best (most fit) individual (Q_c) and the worst (least fit) individual (Q_x) in each subgroup. Update (Q_x) in each subgroup by equations (3, 2). By cross operation, the new (Q_x) is converted to binary (Q_x) by equations (4, 5).
- Step 5: Calculate the evaluation function value for each individual and find the globally fittest individual (Q_h).

5. Testing and Training

After the feature selection, the dataset is divided into two subsets, the training subset and test subset. The perfect selection to testing and training data improves the accuracy of classification. The training of the proposed IDS system using a dataset involves determining various normal and abnormal behavior of attack. The training time is called a convergence rate and it has to be measured multiple times in the network. After the training phase, the proposed IDS system involves testing using the test data. The involved testing data is most of the cases is smaller than the training data for mor detection accuracy. In the proposed system, 70% of the dataset is used for training and 30% is used for testing. The training phase takes 1000 epochs to complete. Also, the training and testing data had the same regularity for the intrusion detection model to achieve the highest performance.

6. Classification

The anomaly detection is represented in a form of a classification process to reduce the potential damage of the network. The hybrid-based attack classification method named as LCNN-GRNN is proposed in this paper. In this hybrid IDS system, various processing layers are involved to classify

the attacks namely the input layer, bi-directional recurrent layer, attention layer, and classification layer. Firstly, the input layer is used to reduce the vector-based representation. The represented vector is transformed to the Bi-directional recurrent layer to analyze the local features. Then the attention layer determines the higher weights to identify key factors to detect anomalies. Finally, the classification or output layer determines the attacks presented in the network.

In the input layer, the numerical values are transformed into encoding vector $\boldsymbol{y_t}$ and the embedding matrix defines M. $\boldsymbol{y_t}$ is computed by:

$$\boldsymbol{y_t}=\mathrm{M}\ \mathbf{x_i} \tag{9}$$

RNN uses a sequence of information and maintains its characteristics over the middle layer. It allows multiple convolutions in the same network at various time steps. The obtained encoding vectors are fed into a bi-directional recurrent layer where $\boldsymbol{y_t}$ and $\boldsymbol{r_{t-1}}$ defines the previous step of hidden state that are input sequence of time t. $\boldsymbol{e_t}$ represents 'forget gate' that detects the discarded information from cell as follows:

$$e_t=\sigma\ (M_e\cdot\ [r_{t-1},\ y_t]+a_e) \tag{10}$$

The 'input gate' determines whether the information should be updated, and generates a new D_t candidate value vector through the tanh layer as given in equations (11) and (12).

$$i_t=\sigma\ ((M_i\cdot\ [r_{t-1},\ y_t]+a_i) \tag{11}$$

$$D_t=\ \mathrm{tanr}\ (M_D[r_{t-1},\ y_t]+a_D) \tag{12}$$

The old cell state is R_t multiplied by e_t that is computed by :

$$R_t=e_t\cdot R_{t-1}+i_t\cdot R_t \tag{13}$$

$$Q_t=\sigma(\mathrm{Mo}\cdot[r_{t-1},\ y_t]+\ a_Q) \tag{14}$$

σ represents the sigmoid function and tanr represents a hyperbolic tangent function,

$$r_{t=}Q_t\cdot\ \mathrm{tanr}(R_t) \tag{15}$$

D_t defines the memory representation and r_t defines the hidden layer at time t. It returns two hidden states such as forward direction and backward direction.

$$r_{forward}=\ (\underset{r_1,}{\rightarrow}\underset{r_2,\ldots.}{\longrightarrow}\underset{r_n,}{\rightarrow}\ ) \tag{16}$$

$$r_{reverse}=\ =\ (\underset{r_1,}{\rightarrow}\underset{r_2,\ldots.}{\longrightarrow}\underset{r_n,}{\rightarrow}\ ) \tag{17}$$

$$r_{t=(}\underset{r_1,r_1,}{\rightarrow\leftarrow}) \tag{18}$$

$$\mathrm{r}\ =\ \{\ r_1,r_2,\ldots.,\ r_n\} \tag{19}$$

The attention layer assigns different weights to local features and this layer output is given to the output layer. The final classification layer detects the prediction probability of all features.

$$\mathrm{u(j=K|\ o)}=\frac{\exp\ (m_k^T\mathrm{o}+\ a_k)}{\sum_{k\prime=1}^{k}\exp(\ (m_k^T\mathrm{o}+a_{k\prime})} \tag{20}$$

Here, "a" represents the bias, and "k" represents number of target classes.

7. Results and discussion

This section describes the dataset used for performance measure as well as the performance criteria. The performance measures used in this section are accuracy, false-positive rate, and True positive rate.

7.1. Performance Measures Criteria

True Positive Rate (TPR): The correlation between the amount of correctly expected attacks and the actual number of attacks is determined. If all intrusions are observed then TPR is 1 which is exceptionally unusual for an IDS. TPR is also named Detection Rate (DR) or Sensitivity. The TPR is represented mathematically as:

$$TPR=\frac{TP}{TP+FN} \tag{21}$$

False Positive Rate (FPR): It is the correlation between the number of normal instances wrongly reported as an attack to the overall number of normal instances is determined. FPR is computed using the following equation:

$$FPR = \frac{FP}{FP+TN} \quad (22)$$

False Negative Rate (FNR): False negative implies when a detector fails to recognize the attack and label an anomaly as normal. Mathematically, FNR is represented as:

$$FNR = \frac{FN}{FN+TP} \quad (23)$$

Classification rate (CR) or accuracy: CR tests how reliable the IDS is to identify normal or abnormal traffic behavior. It is defined as the percentage for all instances correctly predicted as follows:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (24)$$

7.2. Dataset Description

The NSL KDD dataset [24] is used for performance measure of the proposed IDS system in this paper. KDD dataset **contains** millions of records in which 5 million records are used for training and 0.5 million records are used for testing. The dataset is managed by MIT Lincoln Laboratory. The main task is to build a predictive model between bad connections (intrusions or attacks) and good connections (Normal). The data contains a standard group of data that includes a high range of intrusions in a network environment. Each network connection consists of 41 features with the details of time and Window-based features and basic TCP features. In this dataset, the attacks are divided into certain types as given in table 1. the table shows the attack type and its percentage in the dataset as well as its name.

Table 1. Representation of attacks in NSL-KDD dataset

Attacks type	Ratio of attacks	Attack name
Normal	20%	Normal
DoS (Denial of Service)	79%	Neptune, Teardrop,Land,back, Smurf,Pod
U2R	0.01%	Buffer overflow,LoadModule,Perl,Rootkit
R2L	0.19%	Guesspassword,Ftpwrite,Imap,Phf, Multihop,Warezmaster, Warezclient
Probe	0.8%	Portsweep, IPsweep, Nmap, satan

There are various classification methods and machine learning algorithms are trained and tested on the KDD intrusion detection dataset. The normal traffic and DoS attack can easily determine but the determination of other attacks is a challenging task. In the literature, many researchers are failed to determine most of the mentioned attacks.

7.3. Experiment environment

All of the experiments presented in this paper is conducted on the following environment:

- **Processor**: Intel(R) Core (TM) i3– 3.9 GHz
- **RAM**: 8GB RAM
- **CPU:** 64-bit OS, x64-based processor
- **GPU:** Gen8-LP 10/12 EU up to 600MHz
- **OS:** Windows 8.1 Pro N

7.4. Performance Analysis of the Proposed System

As mentioned before, the effectiveness of the proposed method is analyzed using various performance measures, namely accuracy, false-positive rate, and True positive rate. This hybrid IDS system is evaluated with two different NSL-KDD datasets which are KDD Test-21 and KDD Test+. Table 2 shows the average performance details in all of the attack types.

Table 2. Performance measures of the proposed Hybrid IDS system

Method	FPR	Accuracy	TPR	FNR
Proposed-KDD TEST-21	1.4%	92.56%	93.06%	1%
Proposed-KDD TEST plus	0.72%	97.89%	96.11%	0.4%

Table 3. Confusion matrix of the proposed system using KDD Test-21 dataset

Forecasted set of classes\Actual set of classes	DoS	Probe	U2R	R2L	Normal
DoS	2001	94	0	127	170
Probe	155	3989	0	91	107
U2R	0	17	150	11	22
R2L	0	76	92	2222	364
Normal	104	52	33	183	**1780**

Table 4. Confusion matrix of the proposed system using KDD Test+ dataset

Forecasted set of classes\Actual set of classes	DoS	Probe	U2R	R2L	Normal
DoS	6949	74	0	100	735
Probe	51	2324	0	6	40
U2R	0	8	179	5	8
R2L	0	6	6	2640	102
Normal	74	27	14	172	9424

Tables 3 and 4 represent the Confusion matrix of the proposed system for all types of attacks such as DoS, Prob, U2R, R2L, and normal behavior. In this table, the highest values define the attack detection values or true values. The true values are estimated for the proposed system in both KDD Test+ and KDD Test-21 dataset.

7.5. Comparison analysis

After the experimentation of the proposed method, the obtained results are compared to some of the existing systems such as decision tree [25], KNN [26] , multilayer perceptron (MLP) [27], bagging ensemble [28], and a combination of different methods such as Ensemble_DT_DNN-Bag, Ensemble_DT_DNN-Rf_Bag_Boost, Ensemble_Bag_Boost, Ensemble_DT_DNN_MLP_Bag_Boost, Ensemble_Bag_Boost, and Ensemble_DT_MLP_Bag_Boost. The idea behind the combination of different methods is inspired from [23] where the results of each method is extracted by each algorithm and a voting system is applied by the end to take the final decision. We tried to emulate the same configuration of [23] implementing those algorithms including the pre-processing components and its training methodologies. All of those algorithms are implemented for the purpose of comparison with the proposed method. This analysis was made to measure the anomaly detection rate and attack classification rate.

7.6. Anomaly detection rate

In this subsection, the anomaly detection rate is evaluated for all of the algorithms based KDDTest+ and KDDTest-21 datasets.

Figure 3 depicts the comparison of attack detection rate for existing methods and the proposed method using the KDDTest+ dataset. In existing methods, the ensemble_bagging method had the highest detection rate of 86% and the multilayer perceptron contains the lowest detection rate as 74%. Among those existing methods, our proposed system had the highest accuracy of 90.25% in attack detection compared to existing methods. This confirms the results produced by [22] with small enhancement due to the proposed pre-processing operations. This has been also noticed in the following experiments.

Figure 4 represents the comparison of attack detection rate using the KDDTest-21 dataset. In this analysis, again, the ensemble_bagging method contains the highest attack detection rate as 74% and a multilayer perceptron had 45% of lowest attack detection rate. The proposed method has a superior result of almost 90% of accuracy in attack detection using KDDTest-21 dataset.

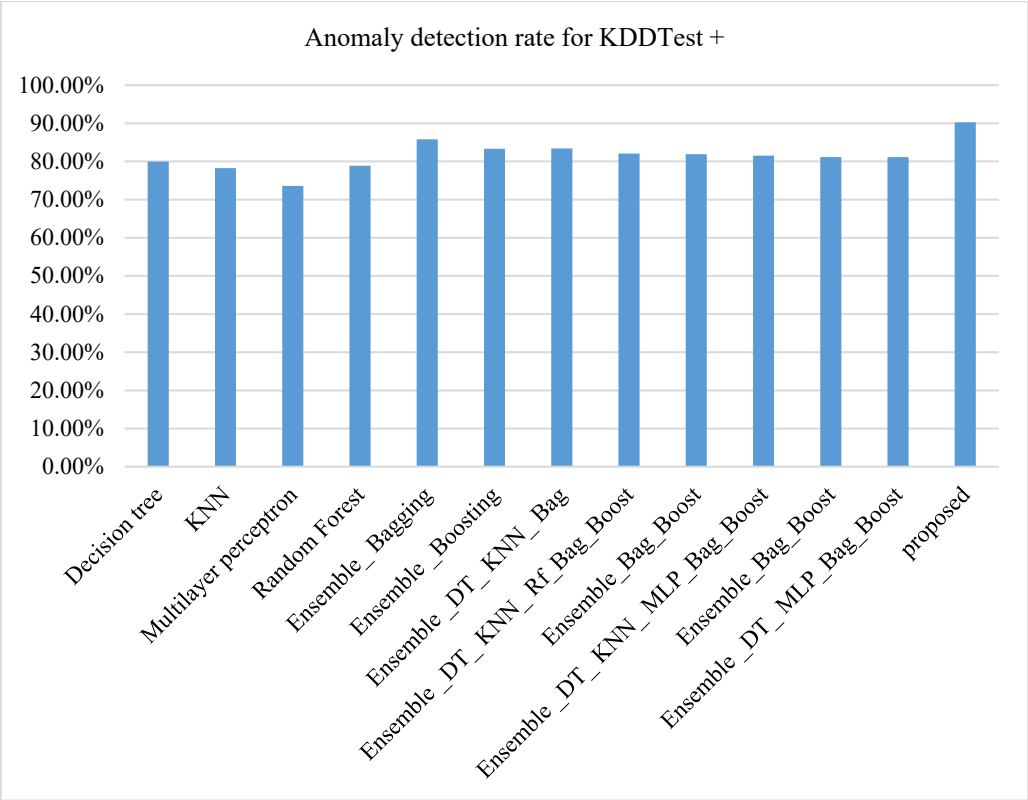

Figure 3. Comparison of attack detection rate using KDDTest+

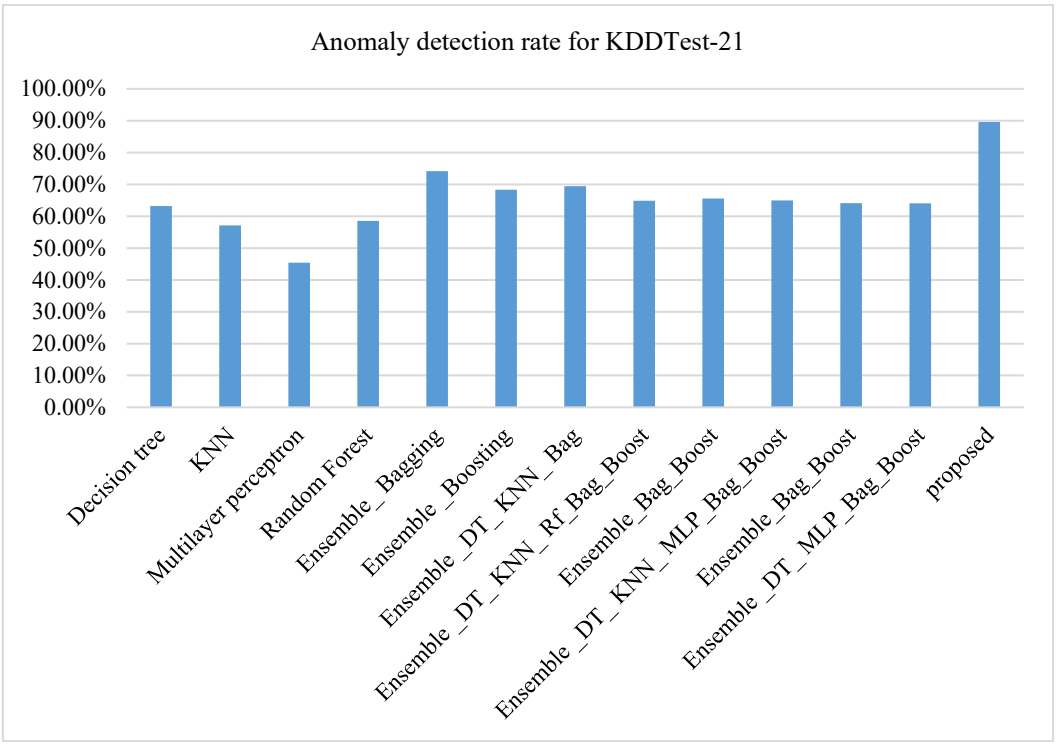

Figure 4. Comparison of attack detection rate using KDDTest-21

7.6.1. Attack classification rate

In this subsection, the set of experiments shows the average classification rate based on KDDTest+ and KDDTest-21 datasets. The classification experiments tend to classify whether the data contains a normal class or abnormal class.

Figure 5 shows the comparison of attack classification rate for existing methods and the proposed method using the KDDTest+ dataset. In existing methods, the ensemble_KNN_MLP_RF method had the highest detection rate of 84% and the Decision tree contains the lowest detection rate

as 69%. Among those existing methods, the proposed system had the highest accuracy of 89% in attack classification compared to existing methods.

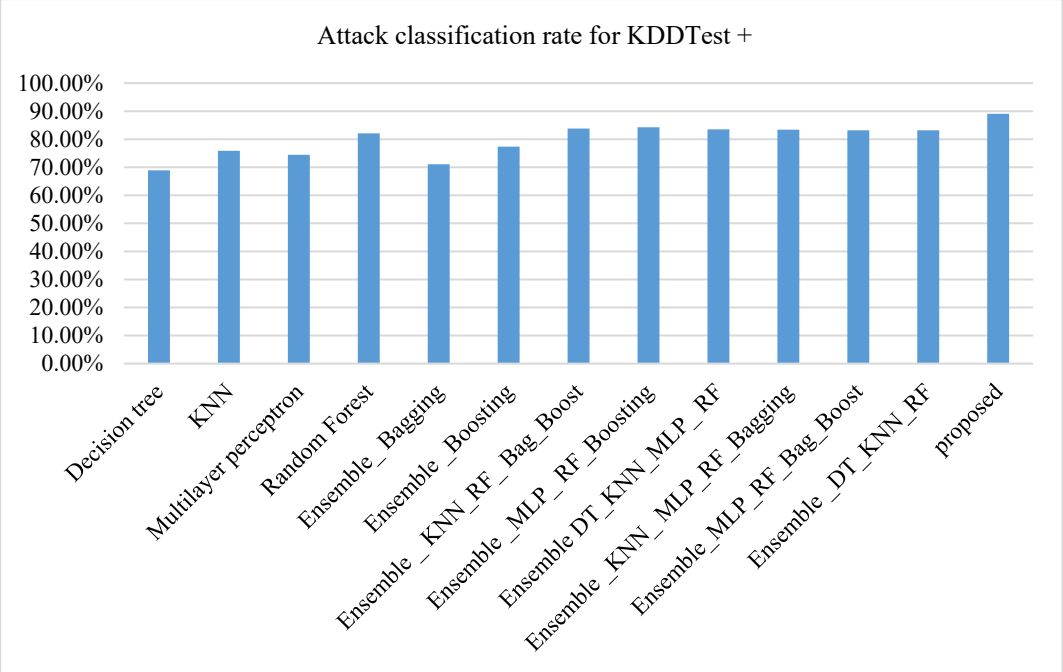

Figure 5. Comparison of attack classification rate using KDDTest+

Figure 6 depicts the comparison of attack classification rate using the KDDTest-21 dataset. In this analysis, the ensemble_KNN_MLP_RF method contains the highest attack detection rate as 79% and the Decision Tree has 56% classification rate which is the lowest attack classification rate. On the contrary, the proposed method provides 91% of accuracy in attack detection using the KDDTest-21 dataset.

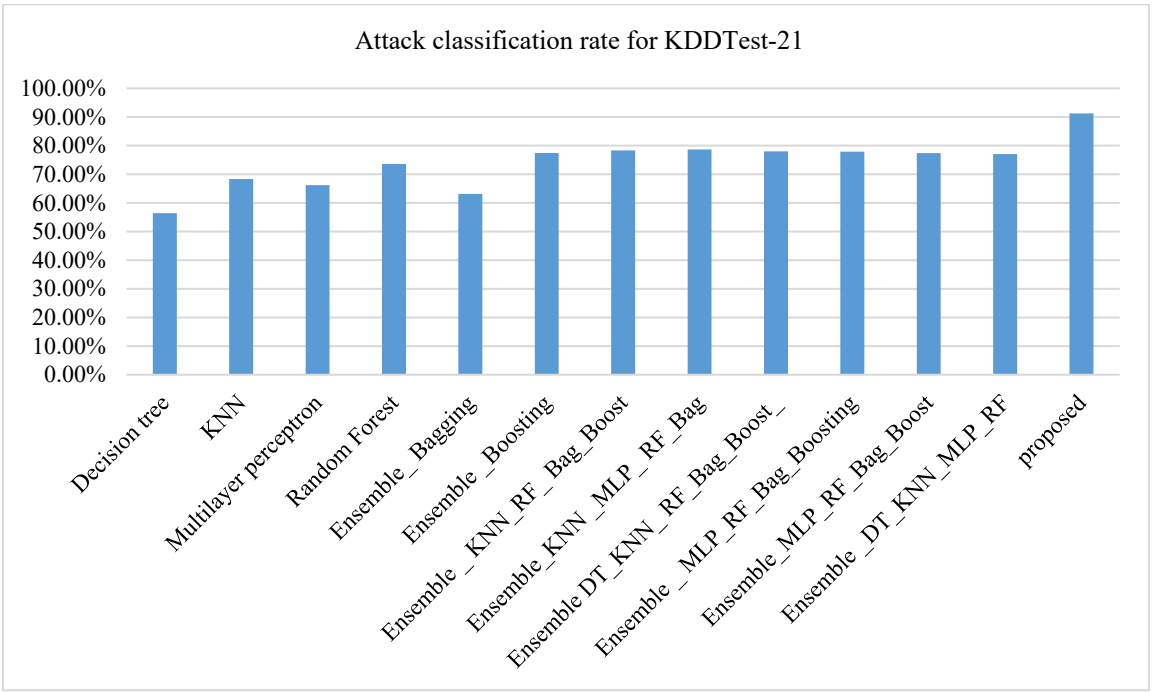

Figure 6. Comparison of attack classification rate using KDDTest-21

8. Conclusion

In this research, a novel hybrid IDS system is proposed to detect the IoT network attacks. The proposed system has two-stage process which are the pre-processing and classification process. From the NSL-KDD dataset, the data preprocessing is done by using encoding, scaling and noise

removal. Then the relevant features are extracted using Enhanced Shuffled Frog Leaping (ESFL) algorithm. The classification process is done by using hybrid IDS system named Light Convolutional Neural Network with Gated Recurrent Neural Network (LCNN-GRNN). This classification determines whether the information is in the normal class or anomaly class. The experimental results showed that the proposed system of superior performance compared to the existing methods. In the future, it is planning to evaluate the clustering-based anomaly detection system with a specialized cloud-based IoT network. In addition, the pre-processing elements proposed in this could be of interest to be impended with other algorithms as well to check if it could be of a benefit to those algorithms.

References

[1] G. D. Putra, V. Dedeoglu, S. S. Kanhere and R. Jurdak, "Poster Abstract: Towards Scalable and Trustworthy Decentralized Collaborative Intrusion Detection System for IoT", Cryptogr. Secur., Feb. 2020.

[2] A. Daia, R. A. Ramadan and M. B. Fayek, "Sensor Networks Attacks Classifications and Mitigation", Ann. Emerg. Technol. Comput., vol. 2, no. 4, pp. 28–43, Oct. 2018, doi: 10.33166/AETiC.2018.04.003.

[3] R. Blanco, P. Malagón, S. Briongos and J. M. Moya, "Anomaly Detection Using Gaussian Mixture Probability Model to Implement Intrusion Detection System", in International Conference on Hybrid Artificial Intelligence Systems, 2019, pp. 648–659, doi: 10.1007/978-3-030-29859-3_55.

[4] R. A. Ramadan, "Efficient Intrusion Detection Algorithms for Smart Cities-Based Wireless Sensing Technologies", J. Sens. Actuator Networks, vol. 9, no. 3, p. 39, Aug. 2020, doi: 10.3390/jsan9030039.

[5] V. Jyothsna, V. V. Rama Prasad and K. Munivara Prasad, "A Review of Anomaly based Intrusion Detection Systems", Int. J. Comput. Appl., vol. 28, no. 7, pp. 26–35, Aug. 2011, doi: 10.5120/3399-4730.

[6] R. A. Ramadan, M. Haidar Sharifa and M. S. Salem, "SIoT: Secure IoT Framework for Smart Environments", in International Conference for Emerging Technologies in Computing, 2020, pp. 51–61, doi: 10.1007/978-3-030-60036-5_4.

[7] S. Fenanir, F. Semchedine and A. Baadache, "A Machine Learning-Based Lightweight Intrusion Detection System for the Internet of Things", Rev. d'Intelligence Artif., vol. 33, no. 3, pp. 203–211, Oct. 2019, doi: 10.18280/ria.330306.

[8] S. Alhaidari and M. Zohdy, "Hybrid Learning Approach of Combining Cluster-Based Partitioning and Hidden Markov Model for IoT Intrusion Detection", in Proceedings of the 2019 3rd International Conference on Information System and Data Mining - ICISDM 2019, 2019, pp. 27–31, doi: 10.1145/3325917.3325939.

[9] B. W. Aboshosha , R. A. Ramadan and A. El-Sayed, "Encapsulate Sec: A Link-Layer Security Architecture for Wireless Sensor Networks", WAS Sci. Nat., vol. 1, 2019.

[10] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques", IEEE Commun. Surv. Tutorials, vol. 21, no. 3, pp. 2671–2701, 2019, doi: 10.1109/COMST.2019.2896380.

[11] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha and K.-K. R. Choo, "A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks", IEEE Trans. Emerg. Top. Comput., vol. 7, no. 2, pp. 314–323, Apr. 2019, doi: 10.1109/TETC.2016.2633228.

[12] E. Hodo, X. Bellekens, A. Hamilton, Dubouilh, P.-L., E. Iorkyase, C. Tachtatzis and R. Atkinson, (2016). Threat analysis of IoT networks using artificial neural network intrusion detection system. In 2016 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1–6). IEEE. https://doi.org/10.1109/ISNCC.2016.7746067

[13] L. Deng, D. Li, X. Yao, D. Cox and H. Wang, "Mobile network intrusion detection for IoT system based on transfer learning algorithm", Cluster Comput., vol. 22, no. S4, pp. 9889–9904, Jul. 2019, doi: 10.1007/s10586-018-1847-2.

[14] D. Midi, A. Rullo, A. Mudgerikar and E. Bertino, "Kalis — A System for Knowledge-Driven Adaptable Intrusion Detection for the Internet of Things", in 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), 2017, pp. 656–666, doi: 10.1109/ICDCS.2017.104.

[15] M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo and A. Robles-Kelly, "Deep Learning-Based Intrusion Detection for IoT Networks", in 2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC), 2019, pp. 256–25609, doi: 10.1109/PRDC47002.2019.00056.

[16] L. R. Parker, P. D. Yoo, T. A. Asyhari, L. Chermak, Y. Jhi and K. Taha, "DEMISe: Interpretable Deep Extraction and Mutual Information Selection Techniques for IoT Intrusion Detection", in Proceedings of the 14th International Conference on Availability, Reliability and Security - ARES '19, 2019, pp. 1–10, doi: 10.1145/3339252.3340497.

[17] 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, doi: 10.1109/ACCESS.2019.2903723.

[18] V. Morfino and S. Rampone, "Towards Near-Real-Time Intrusion Detection for IoT Devices using Supervised Learning and Apache Spark", Electronics, vol. 9, no. 3, p. 444, Mar. 2020, doi: 10.3390/electronics9030444.

[19] S. Murali and A. Jamalipour, "A Lightweight Intrusion Detection for Sybil Attack Under Mobile RPL in the Internet of Things", IEEE Internet Things J., vol. 7, no. 1, pp. 379–388, Jan. 2020, doi: 10.1109/JIOT.2019.2948149.

[20] W. Meng, W. Li, L. T. Yang and P. Li, "Enhancing challenge-based collaborative intrusion detection networks against insider attacks using blockchain", Int. J. Inf. Secur., vol. 19, no. 3, pp. 279–290, Jun. 2020, doi: 10.1007/s10207-019-00462-x.

[21] M. A. Ferrag, L. Maglaras, A. Ahmim, M. Derdour and H. Janicke, "RDTIDS: Rules and Decision Tree-Based Intrusion Detection System for Internet-of-Things Networks", Futur. Internet, vol. 12, no. 3, p. 44, Mar. 2020, doi: 10.3390/fi12030044.

[22] C. Wu, Y. Liu, F. Wu, F.Liu, H. Lu, W. Fan and B. Tang, "A Hybrid Intrusion Detection System for IoT Applications with Constrained Resources," International Journal of Digital Crime and Forensics, vol. 12, no. 1, p. 109–130, 2020. doi: 0.4018/IJDCF.2020010106.

[23] P. Illy, G. Kaddoum, C. M. Moreira, K. Kaur and S. Garg, "Securing Fog-to-Things Environment Using Intrusion Detection System Based On Ensemble Learning", Jan. 2019, doi: 10.1109/WCNC.2019.8885534.

[24] UNB, "NSL-KDD dataset." Available: https://www.unb.ca/cic/datasets/nsl.html. [Accessed: 12-Sep-2020].

[25] K. Peng, Victor C. M. Leung, Lixin Zheng, Shangguang Wang, Chao Huang, and Tao Lin, "Intrusion detection system based on decision tree over big data in fog environment" Wirel. Commun. Mob. Comput., 2018.

[26] Y. Liao and R. V. Vemuri, "Use of k-nearest neighbor classifier for intrusion detection" Comput. Secur., vol. 21, no. 5, pp. 439–448, 2002. doi: 10.1016/S0167-4048(02)00514-X

[27] J. Esmaily, R. Moradinezhad and J. Ghasemi, "Intrusion detection system based on Multi-Layer Perceptron Neural Networks and Decision Tree", in 2015 7th Conference on Information and Knowledge Technology (IKT), 2015, pp. 1–5, doi: 10.1109/IKT.2015.7288736.

[28] D. P. Gaikwad and R. Thool "Intrusion detection system using bagging ensemble method of machine learning", Int. Conf. Comput. Commun. Control Autom., 2015. doi: 10.1109/ICCUBEA.2015.61

© 2020 by the author(s). Published by Annals of Emerging Technologies in Computing (AETiC), under the terms and conditions of the Creative Commons Attribution (CC BY) license which can be accessed at http://creativecommons.org/licenses/by/4.0.