electronics

Article

A Deep Learning-Based Smart Framework for Cyber-Physical and Satellite System Security Threats Detection

Imran Ashraf [1], Manideep Narra [2], Muhammad Umer [3], Rizwan Majeed [4], Saima Sadiq [5], Fawad Javaid [6] and Nouman Rasool [7,8,*]

[1] Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, Korea; imranashraf@ynu.ac.kr
[2] Indiana Institute of Technology Washington Blvd, Fort Wayne, IN 46803, USA; manideep.narra1@gmail.com
[3] Department of Computer Science & Information Technology, The Islamia University of Bahawalpur, Bahawalpur 63100, Pakistan; umersabir1996@gmail.com
[4] Faculty of Computer Science and Information Technology, Universiti Tun Husein Onn Malaysia (UTHM), Bahru 80536, Malaysia; rizinbox@gmail.com
[5] Department of Computer Science, Khwaja Fareed University of Engineering and Information Technology, Rahim Yar Khan 64200, Pakistan; s.kamrran@gmail.com
[6] Department of Communication and Information Engineering, Xi'an University of Science and Technology, Xi'an 710054, China; fawaddayyal@yahoo.com
[7] Electromagnetic Technology and Engineering Key Laboratory, Nanchong 637000, China
[8] School of Electronic Information Engineering, China West Normal University, Nanchong 637000, China
* Correspondence: engr_nouman77@yahoo.com

Abstract: An intrusion detection system serves as the backbone for providing high-level network security. Different forms of network attacks have been discovered and they continue to become gradually more sophisticated and complicated. With the wide use of internet-based applications, cyber security has become an important research area. Despite the availability of many existing intrusion detection systems, intuitive cybersecurity systems are needed due to alarmingly increasing intrusion attacks. Furthermore, with new intrusion attacks, the efficacy of existing systems depletes unless they evolve. The lack of real datasets adds further difficulties to properly investigating this problem. This study proposes an intrusion detection approach for the modern network environment by considering the data from satellite and terrestrial networks. Incorporating machine learning models, the study proposes an ensemble model RFMLP that integrates random forest (RF) and multilayer perceptron (MLP) for increasing intrusion detection performance. For analyzing the efficiency of the proposed framework, three different datasets are used for experiments and validation, namely KDD-CUP 99, NSL-KDD, and STIN. In addition, performance comparison with state-of-the-art models is performed which suggests that the RFMLP can detect intrusion attacks with high accuracy than the existing approaches.

Keywords: intrusion detection system; security threats; machine learning; cyber-physical security

Citation: Ashraf, I.; Narra, M.; Umer, M.; Majeed, R.; Sadiq, S.; Javaid, F.; Rasool, N. A Deep Learning-Based Smart Framework for Cyber-Physical and Satellite System Security Threats Detection. *Electronics* **2022**, *11*, 667. https://doi.org/10.3390/electronics11040667

Academic Editor: Hung-Yu Chien

Received: 22 December 2021
Accepted: 13 February 2022
Published: 21 February 2022

1. Introduction

Malicious activities and intrusion attacks on local and satellite networks are becoming serious security threats. Both the frequency and intensity of such attacks is becoming increased alarmingly. Consequently, intrusion detection approaches and methods have been regarded as significantly important to safeguard internet resources. As internet-connected devices are increasing, cyber security became more important [1]. Intrusion is a series of actions that invade security policies like integrity and confidentiality [2]. The adversaries attack a network with highly skilled programming tools and target vulnerabilities in the network. Therefore, the intrusion detection approach plays a significant role in monitoring and preventing intrusions in a computing network environment [3].

The National information security vulnerability sharing platform of China reported a 1% annual growth of the vulnerabilities related to security [4]. Of 14,201 total security vulnerabilities, 34.5% include high-risk vulnerabilities. In 2018, the Chinese Internet emergency center claimed that distributed denial of service (DDoS) is more than four thousand on average per year. During denial of service (DoS) attacks, the bulk redundancy of requests overloads the system. Attackers choose common and well-known servers like banks and collapse the system leading to huge financial losses. The reports also reveal that more than two thousand resources are utilized for DDoS attacks initiation, ninety thousand IP addresses of destination, and one million broilers. This indicates that approximately one million devices, mobile or computers, have been controlled by network attackers for illegal activities.

A lot of efforts, from academia and industry, have been carried out to secure large networks from intrusion attacks. An intrusion detection system performs real-time surveillance of data transmission over a network and takes appropriate measures when any suspicious activities are found in network transmission. Conventional intrusion detection systems have many limitations for providing network security with higher false-positive rates. A network security system is also leveraged by the development of artificial intelligence (AI) and machine learning tools. However, machine learning models are facing several challenges such as poor generalization ability when dealing with a new and huge amount of data. Deep learning models need large-sized and good quality data for appropriate training and their use is less explored in the field of cybersecurity [5]. Continuously expanding networks with massive devices and the addition of the satellite network, data security, and data privacy are major problems in the satellite-terrestrial network. Limited resources and computational power of the satellite network as compared to the terrestrial network is an additional challenge. When a satellite node is attacked by an attacker, it is exhausted quickly and difficult to fix. Therefore, efficient intrusion detection methods need to be devised to provide high-level protection for modern networks [6]. Machine learning and deep learning models have been proposed by researchers for designing intrusion detection systems [7–9].

The effectiveness of the machine learning techniques depends upon the dataset containing normal and abnormal trends. KDD-CUP 99 dataset has been extensively used for intrusion detection testing. NSL-KDD is an extended form of the KDD-CUP 99. This study utilizes both datasets to improve and optimize the results of existing studies for intrusion detection systems. These datasets are for terrestrial networks and are not suitable for a satellite network because of the limited resources, different tolerance levels, and high privacy requirements. Therefore, this study also considers the distributed network based on satellite and terrestrial networks for intrusion detection. To prove the adaptive ability and generalization of the proposed framework, it is applied to the STIN dataset. The contributions of this work can be summarized as

- An efficient framework is proposed for intrusion detection that utilizes the ensemble architecture comprising Random Forest (RF) and Multilayer Perceptron (MLP). For final prediction, the soft voting criterion is used.
- Several well-known machine learning models are used for performance comparison including RF, support vector machine (SVM), and logistic regression (LR). Experiments are performed using two datasets for terrestrial network traffic including KDD-CUP 99 and NSL-KDD while the STIN dataset is used for satellite network traffic analysis.
- Performance evaluation of the proposed RFMLP is carried out with state-of-the-art approaches in terms of accuracy, precision, recall, and F1 score.

The rest part of the paper is structured as follows. Section 2 describes the important works related to the current study. The details of the datasets, proposed framework, and machine learning models are presented in Section 3. Section 4 discusses the experimental results and the conclusion is given in Section 5.

2. Related Works

Recent studies in the literature on intrusion detection system shows the improved performance of the machine learning models. The intrusion detection approach involves software and hardware for intrusion detection in a network [10]. An embedded system is deployed to implement security policies on a network level. According to the input data, an intrusion detection approach is categorized into network-based, host-based and hybrid systems. A classification-based intrusion detection model extracts features from the online data. Common approaches used for intrusion detection systems are supervised machine learning models, unsupervised machine learning models, and deep learning models.

In unsupervised learning methods, a large volume of data is grouped in clusters automatically without having labels. However, few labeled data can help in improving the performance in cybersecurity or network security. High accuracy cannot be achieved in this way because of the different nature of unknown attacks. An unsupervised learning technique for intrusion detection has been designed to find clusters based on similarity [11]. Supervised learning models need labels for training and show good results. Traditional intrusion detection methods use machine learning and deep learning models. However, machine learning models did not predict different types of invasion attacks accurately because of the insufficient generalization ability of classifiers. The researchers improved the ability of machine learning models by combining them as a hybrid approach and improved the intrusion detection system. Aburomman et al. [12] applied an ensemble of SVM along with particle swarm optimization (PSO), and k nearest neighbor (KNN). The combination of these techniques significantly improved the classification accuracy. However, the advantage of such a combination is also limited and cannot be maximized. Marteau [13] determined covering similarity on symbolic sequences and separate attacks from normal sequences of system calls. He analyzed three similarity measures for comparison and proved that covering similarity is an important measure of an anomaly in the host-based intrusion detection systems.

High dimensional data in a growing number of intrusions and attacks is a big challenge in the intrusion detection system. In order to reduce time complexity and utilization of resources, an important feature of data needs to be analyzed to reduce dimensions. Hussian et al. [14] proposed SVM for anomaly identification and artificial neural network (ANN) at the second step for misuse detection. Similarly, the authors in [15] reduced data dimensions by applying the PCA-LDA ensemble technique.

Deep learning models [16] and deep hierarchical models [17] have been proposed to learn non-linear relationships of data for malicious attack detection. ANN is applied on the KDD99 dataset for intrusion detection by reducing dimensions from correlation and information gain [18]. The model showed improved results in terms of accuracy. The authors proposed a real-time DDoS attack detection method by applying PCA and multivariate component analysis [19]. Musafer et al. [20] designed a sparse autoencoder for intrusion detection system on a reliable and updated network attacks dataset CICIDS2017. The authors proposed a deep learning model namely a memetic algorithm for abnormal traffic detection and tested it on two well-known datasets that are NSLKDD and KDD-CUP 99 [21]. Feature augmentation has been applied along with SVM to provide an effective intrusion detection framework and achieved robust results in terms of training speed and faulty alarm rate [22]. Multilevel intrusion detection has been applied by researchers for intrusion detection [23]. A novel neural network model has been proposed for intrusion detection to improve accuracy results [24]. The growing network connection and integration of terrestrial networks in satellite networks introduce additional risks and security challenges. DDoS is one of the most common attacks in satellite-terrestrial integrated networks and causes service delays. Many studies have been proposed in the literature for DDoS identification in satellite and terrestrial networks. Mowla et al. [25] proposed a jamming detection method and adaptive strategies based on Q-learning. A traffic surveillance system on traffic related to socket programming using machine learning

models has been proposed in [26]. Dynamic attack detection for DDoS based on fuzzy logic has been developed in [27].

These studies represent research efforts for devising suitable approaches for intrusion detection in satellite as well as in terrestrial networks. A comparative analysis of the discussed research works is provided in Table 1.

Table 1. Comparative analysis of the existing approaches.

Ref.	Methods	Dataset	Contribution	Limitations
[12]	SVM-KNN-PSO	KDD 99	Ensemble model using a weighted algorithm for high accuracy.	Multi-class problem is not handled
[13]	SC4ID algorithm	UNM & ADFA-LD	Abnormal system calls by a novel algorithm with higher accuracy	Attack detection problem with sub-sequences attacks.
[14]	SVM-ANN	NSL-KDD	Hybrid model, high performance	Computational complexity
[18]	Deep learning	KDD-CUP 99 & NSL-KDD	Deep learning with robust results	Low performance for R2L attacks
[19]	MDRA	KDD-CUP 99	Real-time attack detection	Low dimensional data cause errors
[20]	Sparse autoencoder	CICIDS 2017	Uses trigonometric simplexes	Sparsity constraints
[21]	Memetic	NSL-KDD & KDD99	PSO with higher accuracy	R2L attacks have a low detection accuracy
[22]	SVM	NSL-KDD	The logarithmic marginal density ratio	Configuration for different datasets is difficult
[23]	MSML	KDD-CUP 99	Multi-level intrusion detection	Optimization for unknown pattern discovery
[16]	MINDFUL	KDD-CUP 99, UNSW-NB 15, CICIDS 2017	Multi-channel for deep feature learning	Class imbalance leads to lower accuracy
[17]	Deep hierarchical	NSL-KDD & UNSW-NB15	Data balancing using SMOTE	High training time needed
[15]	PCA-LDA-SVM	KDD-CUP 99	Dimensionality reduction	Principal component selection for non-Gaussian
[28]	DT-RFE	KDD-CUP 99 & NSL-KDD	Stacked approach	U2R has low accuracy
[25]	Q learning	CRAWDAD	Federated jamming	Asynchronous communication
[26]	DT, KNN, NB & DNN	KDD-CUP 99, open-stack cloud	Socket programming and Open-Stack firewall	Limited to detection of a small range of DDoS
[27]	Fuzzy logic	DDoS attack (T-shark)	Dynamic DDoS attack detection	Manual setting of iterations for T time

3. Materials and Methods

This section discusses the datasets, machine learning models, and the proposed methodology for intrusion detection.

3.1. Machine Learning Models

Machine learning models are selected based on their performance regarding intrusion detection in terrestrial networks and satellite networks.

3.1.1. Random Forest

RF was introduced by Breiman [29]. In the RF model, N trees are constructed by the model using four-step iteration. In the first step, the bootstrap dataset is used for training purposes which is a part of the real dataset. The second step includes tree construction and the third step involves random selection of attributes. At the last step, the result is finalized using majority voting [30]. Equations (1) and (2) present the workflow of RF.

$$p = mode T_1(y), T_2(y), \ldots, T_m(y) \quad (1)$$

$$p = mode \sum_{m=1}^{M} T_m(y) \quad (2)$$

where p is the final prediction which is calculated by of trees, T_1, T_2, and T_m using majority votes [31].

3.1.2. Logistic Regression

LR is based on the logistic function and makes assumptions on the distribution of data. It is an S-shaped curve that maps values between 0 and 1. The standard logistic function $R \rightarrow (0, 1)$ can be defined as

$$\sigma(t) = \frac{1}{(1 + e^{(-t)})} \tag{3}$$

where e is the base of the natural log and value is the value that is to be transformed. LR assumes the linear relationship between input and output values and, is best to use to find a linear relationship between values. It has been used for intrusion detection by many researchers [32,33].

3.1.3. Support Vector Machine

Support vectors define hyperplane. SVM hyperplane categorizes the text into separate classes which are non-overlapping for classification tasks [34]. SVM has been widely being used in text classification and showing robust results in intrusion detection [35,36]. The model finds hyperplanes that differentiate between classes by increasing the hyperplanes' margin distance. It has low complexity when compared with neural network approaches and is simple in interpretation [37]. For the above reasons, it makes sense to use SVM and LR in the experiment for comparison purposes.

3.1.4. Multilayer Perceptron

MLP is a less-complex deep neural network model and has an adequate classification capability. It is a simple layered structure, where the features are according to the neurons of the first input layer, input data is processed by hidden layers using weights for output layer where output value is presented by neurons. The number of hidden layers and the number of neurons at each layer is selected to get optimal results. For maximizing the training capability, training is performed with suitable hyperparameter values. The weights of the layer are managed by backpropagation that uses gradient descent. Rectified linear unit (ReLU) is utilized by hidden layers and in the last layer sigmoid function is used as an activation named as $f(x)$.

The performance of machine learning models is optimized by fine-tuning several parameters and a complete list of the parameter is provided in Table 2.

$$f(x) = \frac{1}{((1 + e^{(-x)})} \tag{4}$$

Table 2. Hyperparameters for the machine learning models.

Model	Parameters
RF	n_estimator = 200, max_depth = 20, random_state = 50.
SVM	C = 1.0, kernel = 'rbf', degree = 3, gamma = 'scale'
LR	Penalty = 'l2', solver = 'lbfgs'
MLP	Dense (neurons = 300), dense (neurons = 200), dense (neurons = 100), activation = 'relu', dropout (0.5), softmax (4)

3.2. Dataset Description

This study considers three datasets to investigate the performance efficiency of the proposed framework for intrusion detection. The details of KDD-CUP 99 and NSL-KDD datasets are summarized in Table 3. KDD-CUP 99 [38] is a benchmark dataset designed by the KDD competition held in 1999. It has been extensively utilized by researchers in investigating intrusion detection systems. It was prepared over nine weeks by simulating

the network environment of the military and consists of 42 attributes. The dataset comprises 4898 samples for the train set and 311 samples for the test set. The testing set belongs to 14 attack families. The labels are mainly divided into normal and four types of attacks. NSL-KDD [39] is also widely used for evaluating intrusion detection models. Each record of intrusion has symbol features (3 dimensional) and digital features (42 dimensional). The labels are mainly divided into normal, DoS, Prob, U2R, and R2L types of attacks. It contains a total of 125,973 samples in the train set and 22,544 samples in the test set.

Table 3. Detail of classes in KDD-CUP 99 and NSL-KDD datasets.

Class	Description
Normal	User behavior simulate connections.
DoS attack	Resources or services use is denied to authorized users.
Prob attack	Information about the system is revealed to unauthorized entities.
U2R attack	Access to account types of administrators is gained by unauthorized entities.
R2L attacks	Access to hosts is gained by unauthorized entities.

STIN security dataset [40] contains attacks of different types in satellite and terrestrial networks. It contains two types of satellite and nine terrestrial-type attacks. Flow-based features are considered in building the STIN dataset. Table 4 presents the characteristics of the dataset.

Table 4. Detail of STIN dataset.

Domain	Attack Type	Attack Time
Terrestrial attacks	Botnet	15:01→15:10
	Web attack	15:21→15:31
	Backdoor	15:41→15:52
	LDAP DDoS	16:01→16:11
	MSSQL DDoS	16:21→16:30
	NetBIO DDoS	16:41→16:50
	Portmap DDoS	17:01→17:13
	Syn DDoS	17:21→17:32
	UDP DDoS	17:41→17:52
Satellite attacks	Syn DDoS	15:23→15:570
	DUP DDoS	16:52→17:20

3.3. Proposed Methodology

The proposed approach is based on the ensemble of deep learning and machine learning models for intrusion detection, as shown in Figure 1. Ensemble approaches have been applied by researchers to improve the efficacy of various classification tasks.

However, for the said purpose this study combines MLP and RF using soft voting criteria. In soft voting, the result of high probability is considered as the final output. The working of the proposed ensemble model is presented in Algorithm 1.

The soft voting criteria of the proposed model are expressed as

$$\widehat{p} = argmax \sum_{i}^{n} RF_i, \sum_{i}^{n} MLP_i \quad (5)$$

where $\sum_i^n RF_i$ and $\sum_i^n MLP_i$ are the probability values against the test sample. Then, the probability values for each instance by RF and MLP pass through the criteria based on soft voting as presented in Figure 2.

The working of the RFMLP can be discussed with an example. A probability score is assigned to each sample that has passed through the RF and MLP. For example, let the probability value of the RF model be 0.4, 0.7, 0.3, and 0.6 for 4 classes, respectively and the

probability value of the MLP model be 0.5, 0.4, 0.6, and 0.8 for 4 classes, respectively where $P(x)$ presents the probability value of x that ranges from 1 to 4, the final probability will be computed as:

$$P(1) = (0.4 + 0.5)/2 = 0.45$$
$$P(2) = (0.7 + 0.4)/2 = 0.55$$
$$P(3) = (0.3 + 0.6)/2 = 0.45$$
$$P(4) = (0.6 + 0.8)/2 = 0.7$$

The proposed RFMLP predicts the final output by joining the predicted probability values of both models on the highest average probability.

Algorithm 1 Ensembling RF and MLP.

Input: input data $(x, y)_{i=1}^{N}$
M_{RF} = Trained RF
M_{MLP} = Trained MLP
for $i = 1$ to M **do**
if $M_{RF} \neq 0$ & $M_{MLP} \neq 0$ & $training\_set \neq 0$ **then**
$P_{MLP_1} = M_{MLP}.probability(class1))$
$P_{MLP_2} = M_{MLP}.probability(class2))$
$P_{MLP_3} = M_{MLP}.probability(class3))$
$P_{MLP_4} = M_{MLP}.probability(class4))$
$P_{RF_1} = M_{RF}.probability(class1))$
$P_{RF_2} = M_{RF}.probability(class2))$
$P_{RF_3} = M_{RF}.probability(class3))$
$P_{RF_4} = M_{RF}.probability(class4))$
Decision function = $max(\frac{1}{n}\sum_{classifier}(Avg(P_{MLP_1}, P_{RF_1}), Avg(P_{MLP_2}, P_{RF_2}), Avg(P_{MLP_3}, P_{RF_3}), Avg(P_{MLP_4}, P_{RF_4}))$
end if
return final label $\hat{p}$
end for

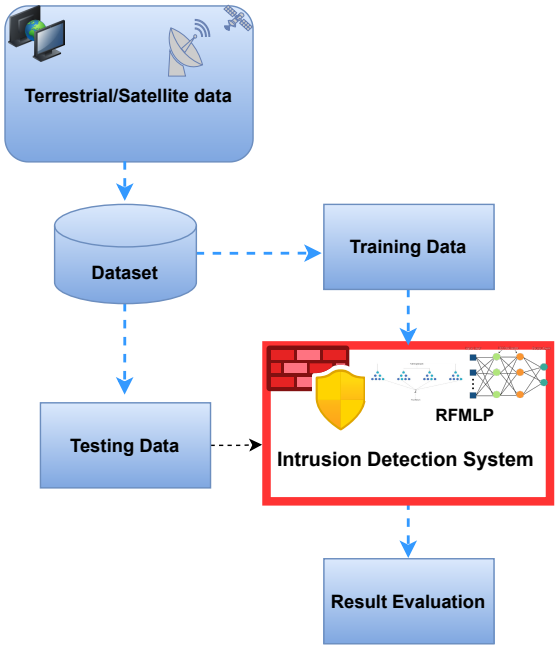


Figure 1. Architecture of the proposed methodology for DDoS attack detection.

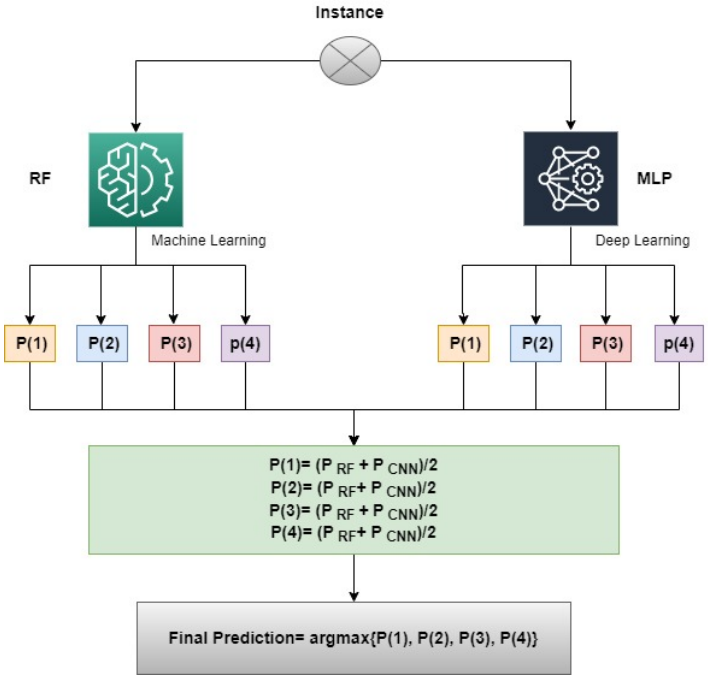


Figure 2. Architecture of the proposed RFMLP model for DDoS attack detection.

3.4. Evaluation Metrics

The performance evaluation of classifiers is commonly computed using evaluation metrics. In this study, accuracy, precision, recall, and F1 score have been used for comparing the performance of algorithms. These metrics are evaluated using a confusion matrix where TP presents True positive, TN shows true negative, FP presents false positive, and FN indicates false negative as shown in the following equations

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{6}$$

$$Precision = \frac{TP}{TP + FP} \tag{7}$$

$$Recall = \frac{TP}{TP + FN} \tag{8}$$

$$F1score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{9}$$

4. Results and Discussion

The proposed ensemble RFMLP is tested on three datasets namely, KDD-CUP 99, NSL-KDD, and STIN to provide high security to both satellite and terrestrial networks.

4.1. Experiment Set Up

Dataset is split into train set and test set in the ratio of 0.7 and 0.3, respectively. The proposed RFMLP is evaluated in terms of accuracy, precision, recall, and F1 score. Experiments are carried out using a 2 GB Dell PowerEdge T430 GPU on 2x Intel Xeon 8 Cores 2.4 GHz machine with 32 GB DDR4 random access memory (RAM). Machine learning and deep learning models are coded in Python programming language in Anaconda Jupyter notebook editor.

4.2. Performance of Machine and Deep Learning Models

Experimental results for machine and deep learning models are presented in Table 5. It can be noticed that traditional machine learning models like RF, LR, and SVM have low accuracy scores than RFMLP for the four attack types. In particular, for the R2L attack

type, the accuracy of RF, SVM, and LR models is significantly lower than MLP and RFMLP models. In addition, LR shows poor performance than the other three models in terms of accuracy. RFMLP has the highest accuracy among all other three models on KDD-CUP 99. The prediction accuracy of RF, SVM, and LR for the R2L attack type is lower than other attack types while RFMLP predicts R2L effectively with a 99.99% on KDD-CUP 99.

Table 5. Accuracy of classifiers on KDD-CUP 99 dataset.

Attack Type	RF	SVM	LR	MLP	RFMLP
DoS	99.82	99.28	96.44	99.99	100.0
Prob	99.12	99.34	98.89	99.98	99.99
R2L	97.21	97.34	97.01	99.26	99.99
U2R	99.16	99.29	99.07	99.89	99.99

Table 6 presents the results for the NSL-KDD dataset for all models. Results indicate that RFMLP outperforms all other models with a significant difference. The performance of RF, SVM, and LR is severely affected by the U2R attack type. Similarly, their performance for R2L attacks is also comparatively poor than DoS and Prob attack types. RFMLP, on the other hand, achieves 100% for DoS and U2R while for Prob and R2L attack types, and its accuracy is 99.98% and 99.97%, respectively.

Table 6. Accuracy of classifiers on NSL-KDD dataset.

Attack Type	RF	SVM	LR	MLP	RFMLP
DoS	99.93	98.82	91.96	100.0	100.0
Prob	98.18	97.73	94.68	99.65	99.98
R2L	97.06	96.94	95.38	99.79	99.97
U2R	94.40	96.64	95.55	99.88	100.0

The performance of all models using the STIN dataset is shown in Table 7 which indicates the RFMLP shows superior performance than all other models. For the UDP_DoS attack type, it obtains a 100% accuracy while its performance is affected for the Syn_DDoS attack type. However, its performance is much better than RF, SVM, LR, and MLP, which obtain 86.18%, 83.37%, 83.42%, and 88.65%, respectively for the same attack type.

Table 7. Accuracy of classifiers on STIN satellite dataset.

Attack Type	RF	SVM	LR	MLP	RFMLP
UDP_Dos	89.45	86.18	86.66	92.17	100.0
Syn_DDoS	86.18	83.37	83.42	88.65	93.18

Table 8 provides the classification results using the STIN terrestrial dataset. Results suggest that the proposed model performs very well by combining RF and MLP. Although a slightly lower performance is observed for 'Portmap DDoS', and 'LDAP DDos' classes with 91.21% and 93.14% accuracy scores, respectively, the overall performance is substantially better than other machine learning models. The low performance for these classes is on account of the low number of samples available for training.

Table 9 presents the performance comparison of RF, SVM, LR, MLP, and RFMLP on all three datasets in terms of accuracy, precision, recall, and F1 score. For traditional models, deep learning-based MLP outperforms the other models in terms of all evaluation measures. However, the performance of the RFMLP is even better than the MLP which shows its significance.

Table 8. Accuracy of classifiers on STIN terrestrial dataset.

Attack Type	RF	SVM	LR	MLP	RFMLP
Backdoor	88.14	85.22	85.48	88.17	96.67
LDAP DDoS	86.11	84.45	84.35	91.21	93.14
MSSQL DDoS	88.45	86.22	87.16	88.36	95.24
NetBIO DDoS	88.45	86.34	86.79	90.41	96.65
Portmap DDoS	87.32	79.99	81.01	89.17	91.21
Syn DDoS	88.21	82.38	82.01	92.34	97.25
UDP DDoS	85.99	84.18	84.17	89.22	97.67

Table 9. Average Accuracy of classifiers on all three dataset.

Model	Dataset	Accuracy	Precision	Recall	F1 Score
RF	KDD-CUP 99	98.92	98.28	97.65	97.96
	NSL-KDD	97.39	97.62	97.45	97.53
	STIN	87.75	89.98	91.02	90.50
SVM	KDD-CUP 99	98.56	99.62	99.62	99.62
	NSL-KDD	97.53	97.78	97.62	97.70
	STIN	84.24	83.35	85.62	84.48
LR	KDD-CUP 99	97.85	97.13	97.65	97.39
	NSL-KDD	94.39	96.61	95.82	96.21
	STIN	84.44	82.18	81.99	82.08
MLP	KDD-CUP 99	98.94	98.99	99.21	98.65
	NSL-KDD	99.83	99.62	99.82	99.72
	STIN	89.24	88.28	92.67	90.47
RFMLP	KDD-CUP 99	99.99	99.99	100.0	99.99
	NSL-KDD	99.99	99.99	99.99	99.99
	STIN	96.24	94.28	98.67	96.47

STIN security dataset consists of different types of attacks from terrestrial and satellite networks. In literature, different techniques have been by researchers that are generally applied on the terrestrial networks and are not appropriate for satellite networks because of different reasons such as limited resources, different tolerance for attacks, limited computational power, and scarcity of datasets for satellite networks. Although the performance of other models is degraded when used with STIN datasets, the proposed RFMLP still performs better as shown in Figure 3. The proposed model is validated using the modern and famous network attack dataset UNSW-NB15. The accuracy score with the UNSW-NB15 dataset is 99.94% which is better than the state-of-the-art approaches [41]. The best performance on these intrusion detection datasets shows the superiority, significance, and reliability of the proposed model.

Figure 4 presents the performance comparison of all models in terms of accuracy on KDD-CUP 99 and NSL-KDD datasets which are the most commonly used datasets to validate the performance of intrusion detection approaches. It can be seen that the result of the proposed RFMLP surpassed the performance of other models. RFMLP shows accurate results for each category of attack including DoS, Probe, R2L, and U2R on the KDD-CUP 99 dataset and proves its good generalization ability.

In addition to conventional performance metrics of accuracy, precision, recall, and F1 score, Mathews correlation coefficient (MCC) has been computed for RFMLP. The proposed model has shown a 0.99 score for MCC, which proves its robustness. Furthermore, the receiver operating curve (ROC) has been drawn for the proposed model. Figure 5 illustrates the ROC curve of the proposed model on KDD-Cup 99, NSL-KDD, and STIN

datasets. The ROC curve also shows the superior performance of the proposed model on all three datasets.

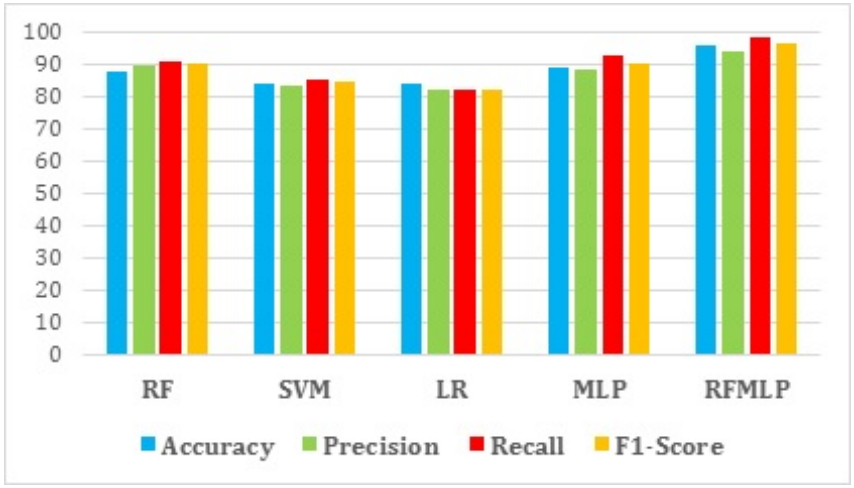


Figure 3. Performance comparison of all models on STIN dataset.

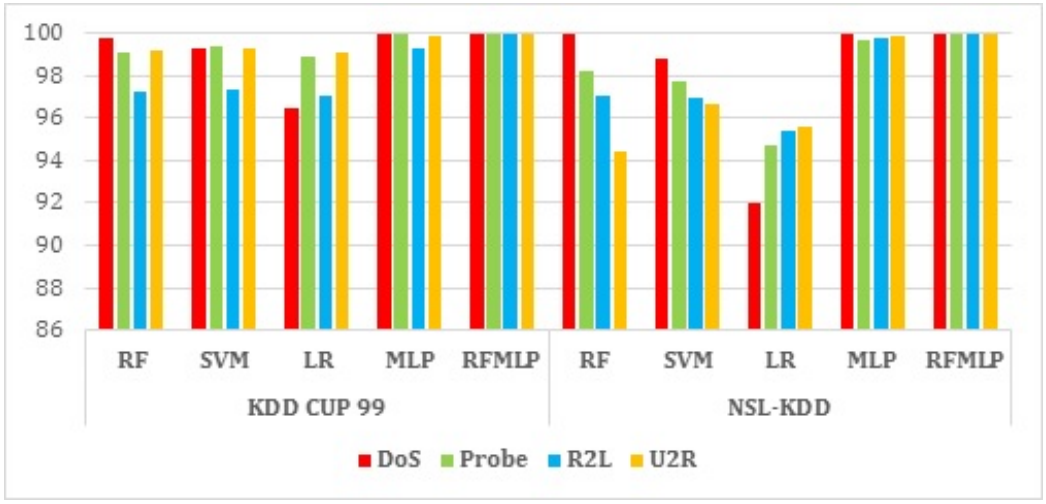
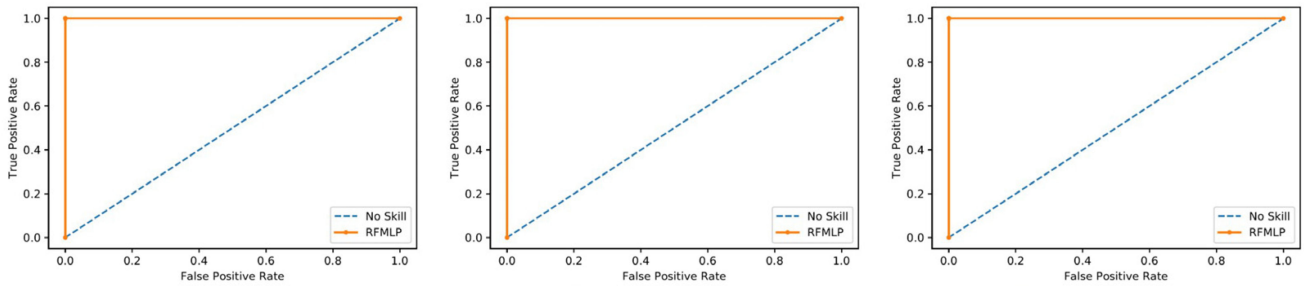


Figure 4. Performance comparison of all models on KDD-CUP 99 and NSL-KDD.



(a) ROC for KDD-CUP 99 (b) ROC for NSL KDD (c) ROC for STIN

Figure 5. The ROC curve of the proposed RFMLP model.

4.3. Computational Complexity of RFMLP Model

The computational complexity of the proposed RFMLP model is estimated using the execution time on all three datasets, and results are given in Table 10. The execution time of the RFMLP is higher than RF, LR, and MLP, however, RFMLP usually takes less time than

SVM. Given that the proposed model takes a slightly longer time for training and testing, the performance of the RFMLP is significantly higher than the machine learning models.

Table 10. Estimated execution time of all classifiers on all three datasets.

Model	Dataset	Estimated Time
RF	KDD-CUP 99	35 s
	NSL-KDD	37 s
	STIN	41 s
SVM	KDD-CUP 99	79 s
	NSL-KDD	93 s
	STIN	135 s
LR	KDD-CUP 99	21 s
	NSL-KDD	33 s
	STIN	47 s
MLP	KDD-CUP 99	38 s
	NSL-KDD	43 s
	STIN	47 s
RFMLP	KDD-CUP 99	43 s
	NSL-KDD	51 s
	STIN	55 s

4.4. Performance Comparison with State-of-the-Art Approaches

Table 11 presents the comparison of the proposed model in terms of accuracy with state-of-the-art approaches from the literature. It can be seen that the proposed RFMLP outperforms the other approaches regarding each category of attacks such as DoS, Probe, R2L, and U2R. Despite combining different approaches like PCA+MCA, SVM-ANN, DT-RFE to improve the performance of classifiers for intrusion detection, RFMLP shows better performance than those models. It can be noticed that the proposed model has shown slightly lower accuracy than SVM-ANN [14] for the 'Prob' class on the NSL-KDD dataset. The proposed model is based on RF and MLP. RF works by combining multiple decision trees and using a bootstrap dataset for training. Occasionally, the bootstrap subset cannot extract the significant features from data due to data scarcity which reduces the performance. However, this problem can be solved by applying upsampling techniques like the synthetic minority oversampling technique (SMOTE) and adaptive synthetic (ADASYN) sampling approaches. The performance of all other classifiers is degraded for R2L and U2R attack types specifically. But the proposed RFMLP shows robust results for the detection of R2L and U2R attack type that shows robustness and generalizability of the approach. Despite this, RFMLP has shown 100% accuracy for DoS and U2R on the NSL-KDD dataset. The proposed RFMLP model is superior in the sense that it is simple with low computational complexity and suitable for both terrestrial and satellite networks.

Table 11. Accuracy comparison of classifiers on KDD-CUP and NSL-KDD datasets.

Ref.	Model	Dataset	DoS	Prob	R2L	U2R	Avg. Accuracy
Proposed	RFMLP	KDD-CUP 99	100.0	99.99	99.99	99.99	99.99
[19]	PCA+MCA		99.99	98.18	97.06	81.82	94.20
[16]	DNN		-	-	-	-	92.49
[28]	DT-RFE		99.76	99.41	97.92	99.74	99.21
Proposed	RFMLP	NSL-KDD	100.0	99.98	99.97	100.0	99.98
[14]	SVM-ANN		100.0	99.99	77.40	88.60	91.48
[17]	Deep hierarchical		96.21	68.56	60.45	61.32	83.58
[28]	DT-RFE		99.74	99.20	98.21	99.77	99.23

4.5. Statistical t-Test

The statistical *t*-Test has also been performed to show the significance of the proposed approach. In the null hypothesis of the *t*-test, H_o shows that the accuracy difference of methods is not significant while alternate hypothesis H_a shows that the accuracy difference is significant. We have performed a *t*-test of the proposed model and the second-best performing model on each dataset. At first, the test is performed on KDD CUP 99 dataset on MLP and RFMLP which shows a 9.22158 value for test statistics and 0.001349 *p*-value. It concludes that the proposed model has improved the performance. Secondly, the test is performed on the NSL-KDD dataset on MLP and RFMLP which shows a 4.9265 value for test statistics and 0.008014 *p*-value. It also proves that the proposed model has improved the performance. Finally, the test is performed on the STIN dataset on RF and RFMLP which shows a 7.10539 value for test statistics and 0.002868 *p*-value. Results prove that the difference is statistically significant with $p < 0.05$ for all three datasets. The proposed model obtained the highest mean rank for accuracy.

5. Conclusions

This study presents a robust and generalized deep learning-based intrusion detection approach for terrestrial and satellite network environments. The increase of network intrusion attacks has also increased the need for an intuitive cybersecurity system to cope with the attacks in the modern network environment. The proposed RFMLP model leverages the advantages of RF and MLP and augments the outputs using the soft voting criterion. The proposed RFMLP model is tested and verified on three datasets, namely KDD CUP 99, NSL-KDD, and STIN. The proposed model improved the classification results and proves its superiority when it is compared with RF, LR, SVM, and other state-of-the-art models from the literature. RFMLP surpassed other models in each category of attacks in terms of accuracy on all three datasets. Detection of R2L and U2R attack types remains a challenge for previous research but the proposed RFMLP shows robust results on these two types of attacks as well. Moreover, the simple architecture of MLP in the proposed ensemble also reduces the computational complexity and makes it suitable for both terrestrial and satellite networks.

Limitations and Future Work

In comparison to the state-of-the-art SVM-ANN [14], the proposed RFMLP model shows slightly low performance for the 'Prob' class from the NSL-KDD dataset. RF bootstrap subset cannot extract the significant features from data occasionally due to data scarcity. This factor, and the low number of samples, can lead to poor performance. In the future, we intend to use SMOTE and ADASYN to further investigate this aspect. In addition, we are planning to deploy appropriate feature reduction techniques in combination with the ensemble model.

Author Contributions: Conceptualization, M.N. and R.M.; Formal analysis, R.M.; Funding acquisition, N.R.; Investigation, M.N. and S.S.; Methodology, R.M., S.S. and M.U.; Project administration,

I.A. and N.R.; Resources, F.J.; Software, S.S. and M.U.; Supervision, N.R.; Validation, F.J. and I.A.; Visualization, F.J.; Writing—original draft, M.N. and M.U.; Writing—review & editing, I.A. All authors have read and agreed to the published version of the manuscript.

Funding: Basic Research Funding of China West Normal Univeristy (Grant Number:21E022).

Acknowledgments: This work is supported by Directorate of Information Technology, Islamia University of Bahawalpur.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Liao, H.J.; Lin, C.H.R.; Lin, Y.C.; Tung, K.Y. Intrusion detection system: A comprehensive review. *J. Netw. Comput. Appl.* **2013**, *36*, 16–24. [CrossRef]
2. Anwar, S.; Mohamad Zain, J.; Zolkipli, M.F.; Inayat, Z.; Khan, S.; Anthony, B.; Chang, V. From intrusion detection to an intrusion response system: Fundamentals, requirements, and future directions. *Algorithms* **2017**, *10*, 39. [CrossRef]
3. Almseidin, M.; Alzubi, M.; Kovacs, S.; Alkasassbeh, M. Evaluation of machine learning algorithms for intrusion detection system. In Proceedings of the 2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY), Subotica, Serbia, 14–16 September 2017; pp. 277–282.
4. Sharma, M. India and China: Warnings Ignored? In *National Cyber Emergencies*; Routledge: Oxfordshire, UK, 2020; pp. 60–75.
5. Andresini, G.; Appice, A.; Malerba, D. Autoencoder-based deep metric learning for network intrusion detection. *Inf. Sci.* **2021**, *569*, 706–727. [CrossRef]
6. Wu, W.; Li, R.; Xie, G.; An, J.; Bai, Y.; Zhou, J.; Li, K. A survey of intrusion detection for in-vehicle networks. *IEEE Trans. Intell. Transp. Syst.* **2019**, *21*, 919–933. [CrossRef]
7. Zhong, W.; Yu, N.; Ai, C. Applying big data based deep learning system to intrusion detection. *Big Data Min. Anal.* **2020**, *3*, 181–195. [CrossRef]
8. Otoum, S.; Kantarci, B.; Mouftah, H.T. On the feasibility of deep learning in sensor network intrusion detection. *IEEE Netw. Lett.* **2019**, *1*, 68–71. [CrossRef]
9. Yang, H.; Wang, F. Wireless network intrusion detection based on improved convolutional neural network. *IEEE Access* **2019**, *7*, 64366–64374. [CrossRef]
10. Tidjon, L.N.; Frappier, M.; Mammar, A. Intrusion detection systems: A cross-domain overview. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3639–3681. [CrossRef]
11. Shojafar, M.; Taheri, R.; Pooranian, Z.; Javidan, R.; Miri, A.; Jararweh, Y. Automatic clustering of attacks in intrusion detection systems. In Proceedings of the 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, 3–7 November 2019; pp. 1–8.
12. Aburomman, A.A.; Reaz, M.B.I. A novel SVM-kNN-PSO ensemble method for intrusion detection system. *Appl. Soft Comput.* **2016**, *38*, 360–372. [CrossRef]
13. Marteau, P.F. Sequence covering for efficient host-based intrusion detection. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 994–1006. [CrossRef]
14. Hussain, J.; Lalmuanawma, S.; Chhakchhuak, L. A two-stage hybrid classification technique for network intrusion detection system. *Int. J. Comput. Intell. Syst.* **2016**, *9*, 863–875. [CrossRef]
15. Aburomman, A.A.; Reaz, M.B.I. Ensemble of binary SVM classifiers based on PCA and LDA feature extraction for intrusion detection. In Proceedings of the 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Xi'an, China, 3–5 October 2016; pp. 636–640.
16. Andresini, G.; Appice, A.; Di Mauro, N.; Loglisci, C.; Malerba, D. Multi-channel deep feature learning for intrusion detection. *IEEE Access* **2020**, *8*, 53346–53359. [CrossRef]
17. Jiang, K.; Wang, W.; Wang, A.; Wu, H. Network intrusion detection combined hybrid sampling with deep hierarchical network. *IEEE Access* **2020**, *8*, 32464–32476. [CrossRef]
18. Manzoor, I.; Kumar, N. A feature reduced intrusion detection system using ANN classifier. *Expert Syst. Appl.* **2017**, *88*, 249–257.
19. Jia, B.; Ma, Y.; Huang, X.; Lin, Z.; Sun, Y. A novel real-time ddos attack detection mechanism based on MDRA algorithm in big data. *Math. Probl. Eng.* **2016**, *2016*, 1467051. [CrossRef]
20. Musafer, H.; Abuzneid, A.; Faezipour, M.; Mahmood, A. An enhanced design of sparse autoencoder for latent features extraction based on trigonometric simplexes for network intrusion detection systems. *Electronics* **2020**, *9*, 259. [CrossRef]
21. Mohammadi, S.; Namadchian, A. A new deep learning approach for anomaly base IDS using memetic classifier. *Int. J. Comput. Commun. Control* **2017**, *12*, 677–688. [CrossRef]
22. Gu, J.; Wang, L.; Wang, H.; Wang, S. A novel approach to intrusion detection using SVM ensemble with feature augmentation. *Comput. Secur.* **2019**, *86*, 53–62. [CrossRef]
23. Yao, H.; Fu, D.; Zhang, P.; Li, M.; Liu, Y. MSML: A novel multilevel semi-supervised machine learning framework for intrusion detection system. *IEEE Internet Things J.* **2018**, *6*, 1949–1959. [CrossRef]

24. Jia, Y.; Wang, M.; Wang, Y. Network intrusion detection algorithm based on deep neural network. *IET Inf. Secur.* **2019**, *13*, 48–53. [CrossRef]
25. Mowla, N.I.; Tran, N.H.; Doh, I.; Chae, K. AFRL: Adaptive federated reinforcement learning for intelligent jamming defense in FANET. *J. Commun. Netw.* **2020**, *22*, 244–258. [CrossRef]
26. Virupakshar, K.B.; Asundi, M.; Channal, K.; Shettar, P.; Patil, S.; Narayan, D. Distributed denial of service (DDoS) attacks detection system for OpenStack-based private cloud. *Procedia Comput. Sci.* **2020**, *167*, 2297–2307. [CrossRef]
27. Alsirhani, A.; Sampalli, S.; Bodorik, P. DDoS detection system: Using a set of classification algorithms controlled by fuzzy logic system in apache spark. *IEEE Trans. Netw. Serv. Manag.* **2019**, *16*, 936–949. [CrossRef]
28. Lian, W.; Nie, G.; Jia, B.; Shi, D.; Fan, Q.; Liang, Y. An Intrusion Detection Method Based on Decision Tree-Recursive Feature Elimination in Ensemble Learning. *Math. Probl. Eng.* **2020**, *2020*, 2835023. [CrossRef]
29. Breiman, L. Bagging predictors. *Mach. Learn.* **1996**, *24*, 123–140. [CrossRef]
30. Sekhar, C.R.; Madhu, E. Mode choice analysis using random forrest decision trees. *Transp. Res. Procedia* **2016**, *17*, 644–652. [CrossRef]
31. Biau, G.; Scornet, E. A random forest guided tour. *Test* **2016**, *25*, 197–227. [CrossRef]
32. Besharati, E.; Naderan, M.; Namjoo, E. LR-HIDS: Logistic regression host-based intrusion detection system for cloud environments. *J. Ambient Intell. Humaniz. Comput.* **2019**, *10*, 3669–3692. [CrossRef]
33. Khammassi, C.; Krichen, S. A NSGA2-LR wrapper approach for feature selection in network intrusion detection. *Comput. Netw.* **2020**, *172*, 107183. [CrossRef]
34. Ribeiro, A.A.; Sachine, M. On the optimal separating hyperplane for arbitrary sets: A generalization of the SVM formulation and a convex hull approach. *Optimization* **2020**, *71*, 213–226. [CrossRef]
35. Tao, P.; Sun, Z.; Sun, Z. An improved intrusion detection algorithm based on GA and SVM. *IEEE Access* **2018**, *6*, 13624–13631. [CrossRef]
36. Wang, H.; Gu, J.; Wang, S. An effective intrusion detection framework based on SVM with feature augmentation. *Knowl.-Based Syst.* **2017**, *136*, 130–139. [CrossRef]
37. Xu, B.; Shirani, A.; Lo, D.; Alipour, M.A. Prediction of relatedness in stack overflow: Deep learning vs. SVM: A reproducibility study. In Proceedings of the 12th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement, Oulu, Finland, 11–12 October 2018; pp. 1–10.
38. Siddique, K.; Akhtar, Z.; Khan, F.A.; Kim, Y. KDD cup 99 data sets: A perspective on the role of data sets in network intrusion detection research. *Computer* **2019**, *52*, 41–51. [CrossRef]
39. Tavallaee, M.; Bagheri, E.; Lu, W.; Ghorbani, A.A. A detailed analysis of the KDD CUP 99 data set. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, 8–10 July 2009; pp. 1–6.
40. Li, K.; Zhou, H.; Tu, Z.; Wang, W.; Zhang, H. Distributed Network Intrusion Detection System in Satellite-Terrestrial Integrated Networks Using Federated Learning. *IEEE Access* **2020**, *8*, 214852–214865. [CrossRef]
41. Singh, P.; Pankaj, A.; Mitra, R. Edge-detect: Edge-centric network intrusion detection using deep neural network. In Proceedings of the 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2021; pp. 1–6.