FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 4 | Pages 1219-1224 | e-ISSN: 2347-470X

An Approach for Identifying Network Intrusion in an Automated Process Control Computer System

Abhijit Das[1] and Pramod[2]
[1]*Research Scholar, VTU, PESITM, Shimoga-577205, Department of CSE, Karnataka, India, abhijit.tec@gmail.com*
[2]*Associate Professor, PESITM, VTU, Shimoga-577205, Department of ISE, Karnataka, INDIA, pramod741230@gmail.com*

***Correspondence:** Abhijit Das; abhijit.tec@gmail.com

ABSTRACT- Technology and networks have improved significantly in recent decades, and Internet services are now available in almost every business. It has become increasingly important to develop information security technology to identify the most recent attack as hackers are getting better at stealing information. The most important technology for security is an Intrusion Detection System (IDS) which employs machine learning and deep learning technique to identify network irregularities. To detect an unknown attack, we propose to use a new intrusion detection system using a deep neural network methodology which provides excellent performance to detect intrusion. This research focuses on an automated process control computer system that recognizes, records, analyzes, and correlates threats to online safety. In addition, two different methods are used to detect an attack (the binary classification and the multiclass classification). One of the most promising features of the proposed technique is its accuracy (98.99 percent with the multiclass classification and the binary classification). The proposed method's first step creates a model for a multiclass intrusion detection system based on CNN. FOA (Fruit Fly Optimization Algorithm) is used in the process's pre-training phase to address the class imbalance issue. Each batch is obtained during the training process using the resampling method following the resampling weights, which are the results of the pre-training procedure.

General Terms: Machine Learning, IDS, Cyber-attacks**.**
Keywords: Intrusion Detection System, ensemble approach, cyber-attacks, CNN, Automated Process Control, FOA.

ARTICLE INFORMATION
Author(s): Abhijit Das and Pramod;
Received: 30/09/2022; **Accepted**: 14/11/2022; **Published**: 25/12/2022;
e-ISSN: 2347-470X;
Paper Id: IJEERSI1202;
Citation: 10.37391/IJEER.100472
Webpage-link:
www.ijeer.forexjournal.co.in/archive/volume-10/ijeer-100472.html

This article belongs to the Special Issue on **Applications of Artificial Intelligence and Internet of Things in Process Control**

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

Computer-related crimes are rising in modern society due to the expanding use of digital technology and web applications becoming more widespread and challenging. New dangers from hackers and the number of cybercriminals is increasing [1], which encourages attackers to take over the entire network infrastructure. Network-based systems are open to malicious intrusions, which might occasionally cause a functional issue. Infiltration is a crucial way that attackers break integrity, availability, and confidentiality. Henceforth, IDS are being used as a defense mechanism to provide security and protection. As a result, they carry out anomaly detection and network attack detection. According to recent studies, IDS' finest data mining solutions are defense mechanisms for identifying attack patterns, which facilitates ongoing observation of the actions carried out within the network. It is meant to prevent unauthorized and malicious behavior if indicated. This application defends against attacks such as Denial of Service (DoS), Remote-to-Local (R2L), Users-to-Root (U2R), and Probe. In order to protect systems against infiltration and to monitor, developed a new security monitoring approach known as a network intrusion detection system [3]. It specifically refers to gathering data from various network nodes of computers or systems. After analysis, it determines if a network has been penetrated or a security policy exploited. Since the 1980s, intrusion detection technology has been extensively researched and is now an essential network security component.

Under network intrusion detection systems, conventional machine learning techniques like Bayesian, Support Vector Machines, Decision Trees, and Logistic Regression are frequently employed. The multiple methods have had positive outputs. However, these algorithms are unsuitable for massive and high-dimensional data because of their sensitivity to outliers and noise. They are unable to address the issue of deteriorated performance of classification. Traditional machine learning techniques have struggled to match user expectations because of the ongoing advancement of digital technology and the expanding variety of cyberattack methods.

Deep learning approaches have recently become popular in several domains, including image identification and natural language processing. These methods have also produced positive results in intrusion detection by combining low-level information. Convolutional neural networks (CNN), recurrent neural networks (RNN), and deep belief networks are the major types of neural networks frequently utilized in intrusion detection. The data flow is broken down into discrete pixel points in bytes, as described in the literature. The images made from the data are then fed into a CNN for convolution, pooling,

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 4 | Pages 1219-1224 | e-ISSN: 2347-470X

and other operations before the classification outputs are obtained [5]. The approach achieves good accuracy with KDD99 datasets in issues involving binary classification and multi-class classifications [6]. The method produced a significant false alarm rate due to the incorrect selection of training parameters during the tests. Still, this method utilized the Short-Term Long Memory (LSTM) network to finish the parameter selection and produced more satisfactory experimental findings.

Accurate detection of numerous threats that have the potential to compromise or harm an information system is known as intrusion detection. An (IDS) may be network or host-based, or it may combine the two. Internal computer monitoring is the main focus of a host-based IDS. A host-based IDS performs various tasks, including file integrity checking, log analysis, and Windows registry monitoring [7]. A network-based IDS keeps track of and examines network activity to look for threats like DoS attacks, SQL injection assaults, and password attacks. Cyberattacks have risen due to the globalization of computer networks and network applications. According to CNBC, a business news program, the average cost of a cyberattack in 2019 was USD 200,000.

IDS can be categorized as a signature-based or an anomaly-based IDS. An IDS with a signature-based approach can only identify known attacks by looking for patterns in those attacks. In order to stay current with all known attack signatures, a signature-based IDS must continuously update its database. On the other hand, an anomaly-based IDS identifies variations from typical traffic behavior.

2. LITERATURE REVIEW

In order to accomplish network intrusion detection utilizing a combination of algorithms, researchers have proposed several approaches. An overview of these combinative strategies that aim to boost performance overall is provided in this section. The use of neutrosophic logic classifier, or an extension of fuzzy logic, was proposed as a new strategy for intrusion detection, including an ensemble design. The genetic algorithm was employed to create the rules. Compared to previous methods, the design, as mentioned earlier, can reduce the false alert rate to 4.19%.

A well-known Support Vector Machine (SVM) classifier may make predictions while classifying from a small collection of examples provided. Using basic security module (BSM) audit data from DARPA's intrusion dataset [8], SVM outperformed ANNs at detecting intrusions. This is because SVM can do great with comparatively little data and run relatively faster than ANN, which needs a lot of training data. SVM is recognized to be particularly good at binary classification; while used in conjunction with different classifiers, it can also produce significant outputs for multiclass classification.

The literature suggested that a hierarchy-based intrusion detection system relies on spatial-temporal characteristics, and the procedure does not consider the issues of fusion of features and data imbalance [9]. Deep convolutional neural networks are used to learn low-level spatial properties of network traffic, then LSTM to understand temporal features. The literature suggests an intrusion detection approach that fuses WaveNet and BiGRU, using the characteristics of WaveNet and the Bidirectional Gated Recurrent Unit (BiGRU) for the feature extraction. It can improve detection accuracy. However, it does not take sample imbalance into account.

The field of study on network security intrusion detection is quite diverse, with existing Convolutional Neural Networks, Adaptive Recurrent Neural Networks, hybrid models, machine learning, and recurrent neural networks. Researchers have used several methods to deal with the issues of low detection accuracy. In intrusion detection, several types of samples are difficult to detect [10]. Most activities involving image and video processing use convolutional neural networks, including image processing, image classification, face recognition, target recognition, and so forth. Additionally, it has seen significant use in intrusion detection in recent years. The recurrent neural network is mostly utilized in connected handwriting tasks, speech, and facial recognition. It is also frequently employed in intrusion detection, thanks to its handling of time series data processing [2]. Emphasized that people who are visually impaired have a hard time navigating their surroundings, recognizing objects, and avoiding hazards on their own since they do not know what is going on in their immediate surroundings. We have devised a new method of delivering assistance to people who are blind in their quest to improve their vision. An affordable, compact, and easy-to-use Raspberry Pi 3 Model B+ was chosen to demonstrate how the proposed prototype works.

A study incorporates sample-weighted and class-weighted techniques into support vector machines to address the issues with intrusion detection. According to experimental findings, the algorithm can benefit from quick response times, high recognition accuracy, lower false alarm rates, and higher classification accuracy in various circumstances.

It suggested a learning model for variation LSTM networks based on a redesigned feature representation to deal with security issues in large-scale data streams [11]. They constructed an encoder neural network with reparameterization to capture low-dimensional elements of the original data. The reconstructed hidden variables are then constrained to a more explicit and understandable form using three loss functions described and quantified. According to experimental data, the model can successfully handle imbalances and high-dimensional difficulties and produce superior detection results. [4] discussed about a system, a low power area reduced and speed improved serial type daisy chain memory register also known as shift Register is proposed by using modified clock generator circuit and SSASPL (Static differential Sense Amplifier based Shared Pulsed Latch). This latch-based shift register consumes low area and low power than other latches. There is a modified complementary pass logic based 4-bit clock pulse generator with low power and low area is proposed that generates small clock pulses with small pulse width.

An approach based on rules has been used in earlier studies to detect cyberattacks. Recently, the focus has shifted to data

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 4 | Pages 1219-1224 | e-ISSN: 2347-470X

mining paradigms and learning from examples [12]. Neural Networks have been widely utilized to distinguish both improper use and strange patterns. New algorithms, support vector machines (SVMs), formed the basis of the kernel, and variants of these are now being proposed to identify cyberattacks. The feature extraction (reduction) technique has increased the classifiers' accuracy.

Although the classifiers mentioned above have enhanced the accuracy of cyber-attack detection, no single classifier can guarantee perfection across all five categories.

3. PROPOSED METHODOLOGY

In any infrastructure or industrial setting, various devices can be networked. *Figure 1* depicts an infrastructure environment for deploying CNN models to analyze malicious activity. An ensemble CNN model processes the data from these infrastructures. When mixed with harmful activities, network communication is disrupted by malware or ransomware, allowing attackers to steal and delete crucial data. We employ an automated process control computer system with proposed ensemble CNN models for malicious activity detection.

The NSL-KDD data is manually classified and then separated into five categories: Normal, DOS, R2L, U2R, and PROBING. *Figure 2* displays the distribution of these five categories of data in the training dataset. We can observe from *figure 2* that Normal data is the type with the most significant amount of data. There are 67344 regular data points. U2R is the type with the fewest data, having only 53 of them. The ratio of data amounts between the two approaches is 1000 to 1. The class imbalance issue will significantly impact Convolutional Neural networks [13]. The system's best accuracy rate can still be 98.9%, even if it cannot recognize U2R assaults. As expected, the optimizer's pursuit of overall accuracy throughout training resulted in an almost 0% detection rate for U2R attacks.

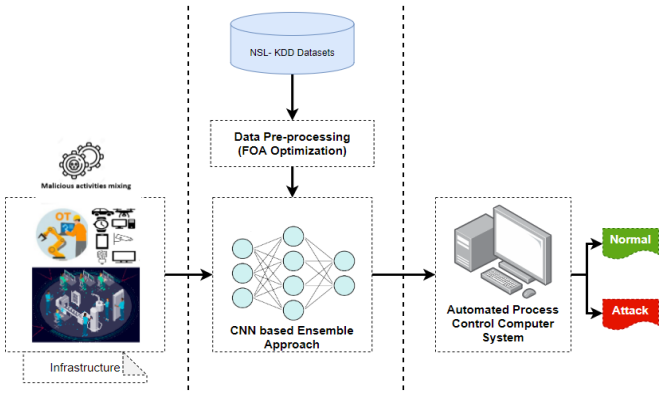

Figure 1: An automated process control computer system for cyber attack

We cannot, however, overlook the capacity of attacks with little training data to be identified because U2R attacks are more dangerous to find. An intrusion detection system is unreliable if it can only spot partial attacks. Contrary to traditional machine learning models, oversampling does not lead to overfitting in CNN. Instead, it is typically used to address data imbalance. However, sampling weights to maximize each attack type's recognition rate might be challenging.

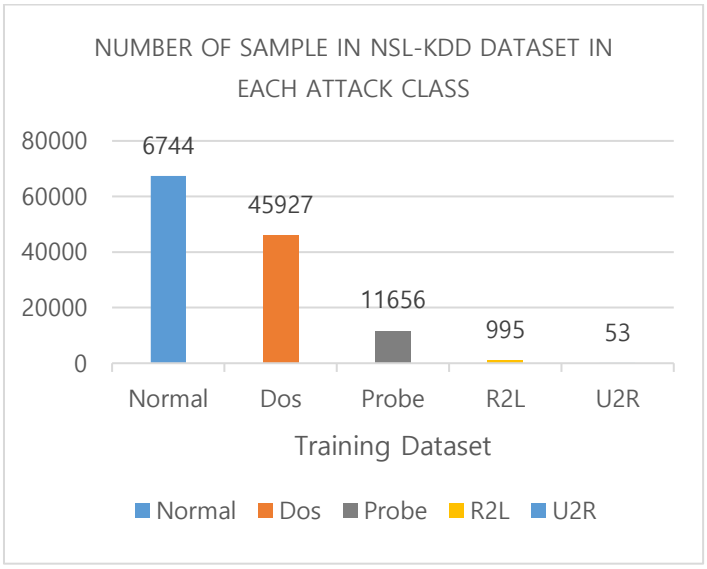

Figure 2: IDS dependent on Convolutional Neural Network

A neural network with a deep structure that performs convolutional is known as a CNN. Convolutional Neural Networks exchange weights in the convolutional layer, significantly reducing the number of weights and boosting efficiency in contrast to conventional fully connected neural networks [14]. Convolutional neural networks are employed in many disciplines, including voice and natural language processing, object location, object following, act assessment, text identification, visual saliency discovery, activity acknowledgment, and scene marking. Convolutional Neural Networks are particularly effective in classifying images. The basic CNN architecture has shown in *figure 3*. The four main layers of a standard CNN are the input layer, convolution layer, pooling layer, and fully connected layer. Each component's specifics are as follows:

3.1 Layers of Convolution

The primary distinction between BP Neural Networks and Convolutional Neural Networks is that they are two types of neural networks with convolutional layers. The convolutional layer's convolutional kernel functions are similar to the filters. We can extract higher dimensional characteristics and do calculations more efficiently by using image processing. [15] This study uses three convolutional layers, which our Convolutional Neural Networks contain. A wide convolution is used in each convolutional layer with no padding for use in convolution computations. The activation function is the ReLU Function.

3.2 Input Layer

Convolutional Neural Network receives its input data mainly from the input layer. The original training data is initially transformed into 8 8 grayscale images for input. We use the grayscale images as the input data for the image recognition

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 4 | Pages 1219-1224 | e-ISSN: 2347-470X

method. The training phase's data were the resampling training data calculated using the FOA weights.

3.3 Pooling Layer

Between two continuous convolutional layers, a pooling layer is allotted to minimize the number of parameters and guard against overfitting. Max-pooling is the pooling technique that is most frequently utilized. Thus, the max-pooling method is also used in this article. The spaces between the three convolutional layers are filled using two pooling layers.

3.4 Fully Connected Layer

All the neurons in a wholly linked layer have connections to neurons in the layers below. The fully connected layer is typically found at the convolutional neural network's tail. Two ultimately linked layers make up the convolutional neural network created in this paper. A random dropout is added to the first completely connected layer so that it can overcome overfitting issues. The Softmax Function is utilized as the classification activation function in the second fully linked layer.

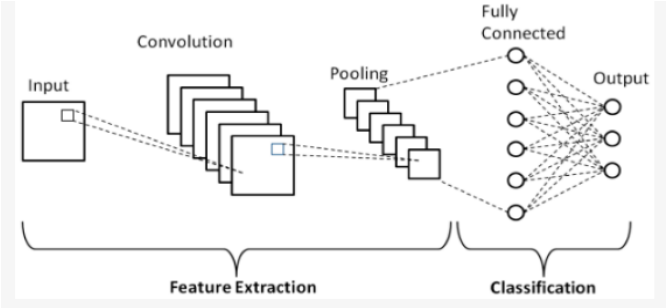

Figure 3: Basic CNN Architecture

4. EXPERIMENTAL RESULT

In tests, we discovered that our approach could not categorize unknown sorts of attacks; thus, we removed them from the test dataset. The steps of the experiment are defined in detail as follows:

All discrete features are initially transformed into a binary vector via the one-hot encoding approach in the data processing phase. After then, all continuous features will have been normalized. The result has been standardized and discretized in units of 0.1. Then, these data will be transformed into a binary vector using the one-hot encoding technique. After the preceding processing, the initial training dataset is transformed into a binary vector with 464 dimensions, which may then be transformed into a grayscale vector with 58 dimensions.

Then, at each grayscale vector, we add 8 zero paddings. Thus, it can be transformed into the example's 8*8 grayscale image.

4.1 Process of Training

The training batch for each epoch is created by resampling the resampling weights collected in the second phase. Cross-entropy is used in the training process as a loss function, and stochastic gradient descent is employed for optimization. Training will end when the accuracy rate has not significantly increased after 30 iterations.

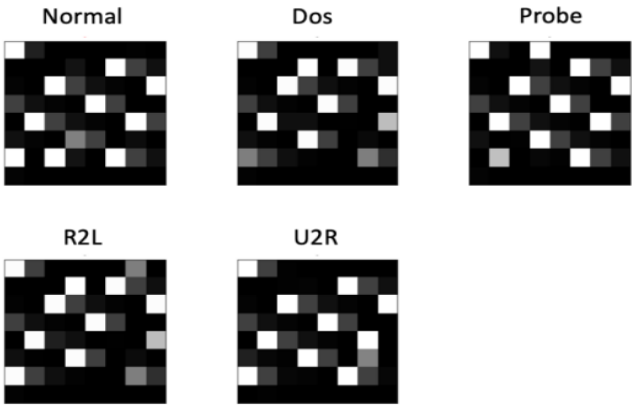

Figure 4: Image of Grayscale of various attacks

5. EVALUATION OF EXPERIMENTS AND RESULTS

$$\text{Recall Score} = \frac{TP}{TP + FN} \quad (1)$$

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

$$\text{F1 Score} = \frac{2 * precision * recall}{precision + recall} \quad (3)$$

The F1, recall, and precision scores are calculated for a list of attack types defined in *figure 4*. The recall rates that correlate to the various attacks that were evaluated as part of the multi-classification task are presented in *table 1*. The objective of this study was to achieve a greater recall rate in intrusion detection. Based on the trial data and the analysis findings, it is possible to conclude that the system achieved an average recall rate of 87.1% across its five classes with the FOA-optimized technique. We can also discover that the recall rate R2L and U2R, the two attack types, have become more effective notably; this implies that when such attacks occur. There is a good possibility that we will be able to identify these attacks successfully. *Table 2* summarizes the comparison of the Precision Score of the experimental findings. They are presented in the context of comparing precision scores using the FOA optimized approach and assuming that the network model remained unchanged. Every performance measure of the proposed model underwent a significant increase in quality when contrasted with the raw data. In addition, the FOA optimized approach that was employed in this work exhibited a certain improvement in the F1 score, as *table 3* demonstrates.

The fundamental problem is that there is excessive variation between the different data categories in the quantity of the test data. Even though less than 0.1% of the data is of the Normal kind, the FP value will increase if it is wrongly classified as the U2R type of the U2R kind. Equation 2 indicates a negative correlation between an increase in FP and a decrease in the Precision Score. The most important consideration. The

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 4 | Pages 1219-1224 | e-ISSN: 2347-470X

capacity of an intrusion detection system to determine when an attack has occurred. The approach suggested in this study presents that the detection system can more easily detect entry attacks. The findings of the evaluation are displayed in *figure 5*.

Table 1: Comparison of recall

	Normal	Dos	Probe	R2L	U2R
FOA Optimized	92.76%	92.27%	91.78%	93.68%	62.45%
Not processed	92.75%	85.34%	87.18%	0%	0%

Table 2: Comparison of Precision Score

	Normal	Dos	Probe	R2L	U2R
FOA Optimized	96.57%	97.78%	82.83%	34.68%	2.5%
Not processed	96.81%	85.22%	86.47%	0%	0%

Table 3: Comparison of F1 Score

	Normal	Dos	Probe	R2L	U2R
FOA Optimized	92.61%	96.25%	87.06%	48.68%	4.61%
Not processed	92.05%	97.01%	86..51%	0%	0%

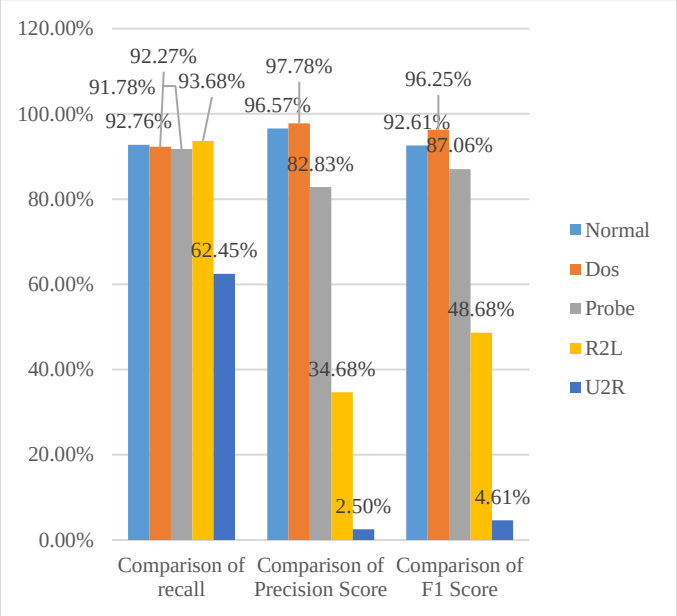

Figure 5: Evaluation results

6. CONCLUSION

This research proposes a convolutional neural network-based intrusion detection system for an automated process control computer system. Both training and testing are conducted using the NSL-KDD dataset. In order to get the optimal training data resampling weights, this work performs a pre-training process using the Fruit Fly Optimization Algorithm to address the class imbalance problem. The issue that cannot identify some attacks owing to the lack of training data has finally been resolved. By removing redundant and unnecessary features from the dataset, the feature selection approach is frequently used to identify the best feature subset and boost system performance.

The Convolutional Neural Network technique avoids the ideal feature selection. Future studies may focus on directly translating network packets into images to get beyond the issue of artificial feature selection. Moreover, the structure suggested in this research can be enhanced as the convolutional neural network evolves quickly [17]. As an illustration, several academics have presented the dropout function, which can lower overfitting and increase accuracy. These procedures can be considered in the subsequent examination to enhance the construction of convolutional organizations. This paper shows that the model has areas of strength for high identification accuracy and a low fake problem rate while handling a large amount of high-layered network information. Although it increases detection accuracy, the model suggested in this paper still has some drawbacks: first, the model has a high number of parameters; second, it takes a long time to run; and third, although it increases detection accuracy for a small number of samples.

7. ACKNOWLEDGMENTS

The authors whose works are cited and included in the references to this manuscript are acknowledged by the authors for their enormous assistance. The authors would also want to express their gratitude to the writers, editors, and publishers of all the books, papers, journals, and other sources used in reviewing and discussing the literature for this work.

REFERENCES

[1] L.; Quan, Y. Dynamic Enabling Cyberspace Defense; People's Posts and Telecommunications Press: Beijing, China, 2018.

[2] Ren, X.K.; Jiao, W.B.; Zhou, D. Intrusion Detection Model of Weighted Navie Bayes Based on Particle Swarm Optimization Algorithm. Comput. Eng. Appl. 2016, 52, 122–126.

[3] Teng, L.; Teng, S.; Tang, F.; Zhu, H.; Zhang, W.; Liu, D.; Liang, L. A Collaborative and Adaptive Intrusion Detection Based on SVMs and Decision Trees. In Proceedings of the IEEE International Conference on Data Mining Workshop, Shenzhen, China, 14 December 2014; pp. 898–905.

[4] Chen, S.X.; Peng, M.L.; Xiong, H.L.; Yu, X. SVM Intrusion Detection Model Based on Compressed Sampling. J. Electr. Comput. Eng. 2016, 2016, 6.

[5] Reddy, R.R.; Ramadevi, Y.; Sunitha, K.V.N. Effective discriminant function for intrusion detection using SVM. In Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur, India, 21–24 September 2016; pp. 1148–1153.

[6] Tao, Z.; Sun, Z. An Improved Intrusion Detection Algorithm Based on GA and SVM. IEEE Access 2018, 6, 13624–13631.

[7] Wang, H.W.; Gu, J.; Wang, S.S. An Effective Intrusion Detection Framework Based on SVM with Feature Augmentation. Knowl.-Based Syst. 2017, 136, 130–139.

[8] Sahu, S.K.; Katiyar, A.; Kumari, K.M.; Kumar, G.; Mohapatra, D.P. An SVM-Based Ensemble Approach for Intrusion Detection. Int. J. Inf. Technol. Web Eng. 2019, 14, 66–84.

[9] Sahu, S.; Mehtre, B.M. Network intrusion detection system using J48 Decision Tree. In Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI), Kochi, India, 10–13 August 2015; pp. 2023–2026.

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 4 | Pages 1219-1224 | e-ISSN: 2347-470X

[10] Jiang, F.; Chun, C.P.; Zeng, H.F. Relative Decision Entropy Based Decision Tree Algorithm and Its Application in Intrusion Detection. Comput. Sci. 2012, 39, 223–226.

[11] Ahmim, A.; Maglaras, L.A.; Ferrag, M.A.; Derdour, M.; Janicke, H. A Novel Hierarchical Intrusion Detection System Based on Decision Tree and Rules-Based Models. In Proceedings of the 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini Island, Greece, 29–31 May 2019; pp. 228–233.

[12] Yun, W. A Multinomial Logistic Regression Modeling Approach for Anomaly Intrusion Detection. Comput. Secur. 2005, 24, 662–674

[13] Kamarudin, M.H.; Maple, C.; Watson, T.; Sofian, H. Packet Header Intrusion Detection with Binary Logistic Regression Approach in Detecting R2L and U2R Attacks. In Proceedings of the Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec), Jakarta, Indonesia, 29–31 October 2015; pp. 101–106.

[14] Kumar, Gulshan. "Evaluation metrics for intrusion detection systems-a study." Evaluation 2.11 (2014): 11-7.

[15] LeCun, Y.; Bengio, Y.; Hinton, G. Deep Learning. Nature 2015, 521, 436–444.

© 2022 by Abhijit Das and Pramod. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).