EAI Endorsed Transactions
on Internet of Things

Review Article EAI.EU

A Review of Machine Learning-based Intrusion Detection System

Nilamadhab Mishra[1, *], Sarojananda Mishra[2]

[1]Engineering, Biju Patnaik University of Technology, Rourkela, Odisha, India
[2]Indira Gandhi Institute of Technology, Sarang, Odisha, India

Abstract

Intrusion detection systems are mainly prevalent proclivity within our culture today. Interference exposure systems function as countermeasures to identify web-based protection threats. This is a computer or software program that monitors unauthorized network activity and sends alerts to administrators. Intrusion detection systems scan for known threat signatures and anomalies in normal behaviour. This article also analyzed different types of infringement finding systems and modus operandi, focusing on support-vector-machines; Machine-learning; fuzzy-logic; and supervised-learning. For the KDD dataset, we compared different strategies based on their accuracy. Authors pointed out that using support vector machine and machine learning together improves accuracy.

Keywords: Intrusion Detection, Machine Learning, Support Vector Machine, Dataset Attacks

Received on 11 December 2023, accepted on 01 March 2024, published on 07 March 2024

doi: 10.4108/eetiot.5332

*Corresponding author. Email: nilamadhab76@gmail.com

1. Introduction

Nowadays in the world, the big concern is the castle. As the internet networks used rapidly, accordingly the attackers also grown exponentially alike [1][2][3]. As a result, network security requires intrusion detection systems to avoid intruders from accessing information. Continuously monitoring network system for off base attitude through hardware or software by intrusion-detection-system (IDS) which afford timely alarm to the system administrators. Intrusion detection devices track all entering and outgoing traffic and exercises to identify possible intruders.

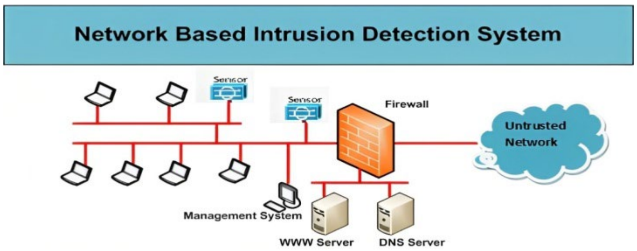

Figure 1. Intrusion Detection System of Network

Deep learning algorithms are implemented to detect intrusion. Machine-Learning processed the raw facts and develop the diagnostic models [4][5]. It has grown rapidly over the past 20 years, providing powerful methods and techniques for a variety of fields [6][7].

This document proposes the use of the NSL-KDD record, and the updated dataset of Kdd_Cup_99 contains the record of the network. This was produced to address issue specific to KDD CUP. [12]. Classify the data using help vector machines [13]. It transforms the data using techniques known as kernel tricks and finds ideal bounds between potential outputs based on these transformations [14][15].

In view of that, anomaly based, signature based, and hybrid-based type NIDs are three types of the network intrusion detection systems (NIDs) represented in Fig 2. The NIDS attempts to prevent different attacks like DoS (Daniel of Service attack), scanning of port on the computer itself or computer networks. Some of the attacks are taking shape mutely to get originated and stay within the local computer networks or reside in the remote source which is the out of the network. Efficiently the NIDS is adopted in a firewall which is identified and protect the attacks from known sources. On the basis of operations

NIDSs classified into offline and online NIDS, also otherwise known as tap mode and inline mode. Formerly the rule based real time system which later deal with the stored data and implement specific logic for decision making to recognize attacks.

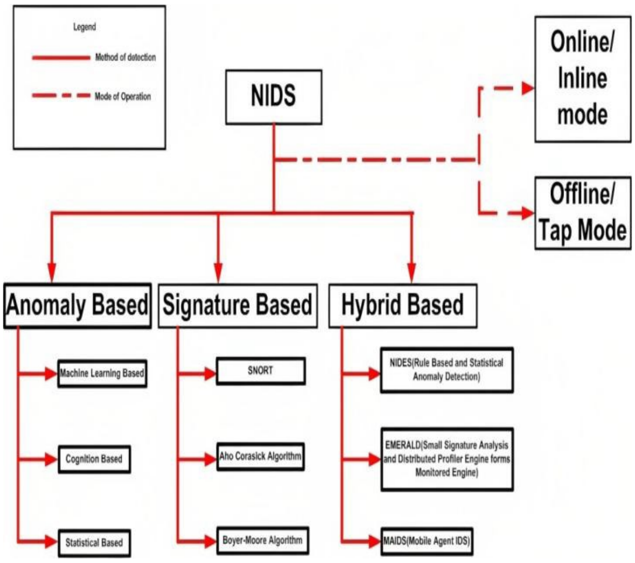

Figure 2. NIDS-Classification

Table 3 demonstrates the description of different methods as well as their computed precision. The table below shows the forms of attacks and their names, with attacks falling into four groups.

Table 1. Categories of Attacks

Sl.No	Categories of Attacks	Attack Description
1	user-to-root attack (u2r):	In local computer illegal way into the super-user or root accounts.
2	remote-to-local attack (r2l):	In the whole networks illegal access to a wounded machine.
3	denial of Service attack(dOs):	Disallow justifiable requests to a system
4	probe:	Attack Information which gathered attack.

In the NSL-KDD dataset, several protocols are used in the NSL-KDD, as seen below [16][17][18].

Table 2. Train and Test Sample dataset of Kdd_Cup

DATASET	tcp	udp	icmp
KDD_Train+20%	20,526	3011	1655
KDD_Train+	1,02,689	14993	8291
KDD_Test+	18,880	2621	1043

2. Literature Survey

To make the algorithm more efficient, the author of proposed supervised learning of K-NN and unsupervised learning of k-means algorithms to inn the weighted data packets and also for selection of features [1]. He also claims that the proposed approach has similar results for detecting all attack types, which improves u2r performance of classification, which make confused to detect intrusion.

[2] Focused on anomaly-detection suggested an IDSs. To evaluate whether network traffic is normal or attack, this projected method involves data alteration, normalization, related feature collection, as well as a uniqueness finding form founded a classifier on SSPVSSVD (Satisfiability-Solvers and Software-Verification Sparse-Single Value-Decomposition) and a solver on SMD (short-message-delivery). They reviewed the IDS on the entire dataset and includes training nodes.

In [3], the researcher suggested a method for using data mining in network security settings such as intrusion detection systems, in which the HFSA is combined with the Nave-byes-multinomial technique. Then, further compares categorization efficiency in the form of accuracy, correctness, and memory, as well as a portion of existing recognition approaches. These sustain delivery execution while simultaneously dramatically reducing computational time and expense.

The techniques safe allowed virtual quality routing (SEVQ) were suggested by the author in [4] for network points to approximate and define the effect of obstruction, and for a resource point to integrate this approximation into its interchange allotment. The author introduced a more effective method of deploying IDSs on each node of a mobile-adhoc-network. To test the assessment system, compare the performance of IDSs with two scenarios: at first maintaining IDSs operation during the imitation period, and secondly use the suggested system to minimize the active time of IDSs at each node in the set-up.

At first offering an appropriate dataset-preprocessing technique, researchers suggested a genetic-algorithm (GA IFS) with increased efficient feature selection to classify anomaly in the system [5]. The dataset preprocessing strategy used in his paper was able to reduce training data by 79.07 percent and test data by 80.47 percent.

The author of [6] suggested a discretization function mechanism that is used solely to make the assessment-making process for hysterically valued features easier. Number of machine-learning algorithms and feature-selection methods that are worn to investigate their impact on interruption finding accuracy and time. This result indicates the increased the pace of the research using feature-selection algorithm for accuracy.

In [7], the author suggested hybrid methods that incorporate techniques such as J48 and Decision-Tree, Support-Vector-Machine, and Nave-Bayesian for the identification of various types of assault, as well as dissimilar variety of precision depending on algorithms. Both experiments were performed on the nsl-kdd dataset.

To identify various attack types, [8] employs a variety of classifiers, including DCNN (Deep-Convolution Neural-Network), RF (Random-Forest), and NAÏVE-BAYESIAN. The author of the study makes a distinction between minority and majority categorization and comes to the conclusion that improper minority detection might cause some anomalies in the IDES (Intrusion Detection Expert System).

[9] proposed a model-based Anomaly-based intrusion detection technique called OPSO-PNN (Oppositional Particle Swarm Optimization- Probabilistic Neural Network). Evaluation between this representation and PSO-PNN, PSO-RB, and PSO-PNN was performed using the standard NSL and KDD dataset. Known anti-Particle-Swarm Optimization-Probabilistic Neural-Network provides improved classification compared to PSO-PNN. It was more accurate and had a higher detection rate with a fairly low false positive rate.

Researchers [10] proposed Deep Belief Network (DBN), which analyzed and extracted assault identifiers from complex facts, and State Sustaining Extreme Machine Learning (SPELM). The accuracy of attack detection is increased by SPELM, which can distinguish between normal and attack nodes. He also comes to the conclusion that State Preserving Intense Machine Learning outperforms Deep Belief Networks.

The author of [11] proposed an improved hybrid-intrusion detection system technique based on FCM (Firebase-Cloud Messaging) and SVM (Support-Vector Machine). In his work, this method helped reduce the complication of huge data sets and increase the effectiveness of support-vector machine classifiers. To do this, first group the pre-processed training dataset using Firebase Cloud Messaging before adding feature information value ratios. for every group whose entropy exceed a certain brink, a support vector machine classifier is created to more accurately determine the type of attack.

Ghosh et al.'s 2023 study [12] focuses on "Water Quality Assessment Through Predictive Machine Learning", highlighting the use of machine learning for analyzing and predicting water quality parameters. In "Unraveling the Heterogeneity of Lower-Grade [13] Gliomas," Rahat, Ghosh, and colleagues (2023) delve into deep learning-assisted segmentation and genomic analysis of brain MR images, offering new insights into this medical condition. Potato Leaf Disease [14] Recognition and Prediction using Convolutional Neural Networks," by Ghosh, Rahat, and team (2023), showcases the application of convolutional neural networks in accurately identifying diseases in potato leaves. Mandava, Vinta, Ghosh, and Rahat's [15]2023 research presents "An All-Inclusive Machine Learning and Deep Learning Method for Forecasting Cardiovascular Disease in Bangladeshi Population", integrating advanced AI techniques for health predictions. The 2023 study by Mandava et al., titled "Identification and Categorization of Yellow [16] Rust Infection in Wheat through Deep Learning Techniques", applies deep learning methods to detect and categorize wheat infections effectively. Hasim, Rahat, Ghosh, and colleagues' 2023 article, "Using Deep [17] Learning and Machine Learning: Real-Time Discernment and Diagnostics of Rice-Leaf Diseases in Bangladesh", explores AI-based solutions for diagnosing rice-leaf diseases. Deciphering Microorganisms through Intelligent Image Recognition", authored by Khasim, Ghosh, Rahat, and others in 2023, discusses [18] the use of machine learning and deep learning in identifying microorganisms through advanced image recognition techniques. The 2023 study by Mohanty, Ghosh, Rahat [19] and Reddy, "Advanced Deep Learning Models for Corn Leaf Disease Classification", focuses on the application of deep learning in classifying diseases in corn leaves based on a field study. Alenezi and team's 2021 research, "Block-Greedy and CNN Based Underwater Image Dehazing[20] for Novel Depth Estimation and Optimal Ambient Light", investigates novel CNN-based methods for enhancing underwater image clarity and depth estimation.

Table 3. Literature Analysis

Sl.No	Reference	ACCURACY%			
		U2R	R2L	DO S	PROB E
1	[1]	70.8	97.6	94.3	98.17
2	[5]	98.2	94.9	97.2	95.11
3	[7]	97.5	97.7	98.1	97.6
		93.4	93.7	97.5	97.1
		71.1	69.9	74.2	73.9
4	[8]	45	31	61	59
		67.3	86.6	93.2	97.44
		95.5	52.2	100	98.43
5	[10]	53	52	53	48
		93	92	95	92
6	[11]	65	90	98.4	95
7	[12]	92	91	93	98.8
		98	93	92	82
		99.9	98	98.9	95
		99.9	92	98	97

3. Background

Thanks to a new approach called machine learning, computers can learn by themselves from previous data. Machine learning uses a variety of approaches to create mathematical models to predict the future based on past data and expertise. Some argue that the branch of artificial intelligence known as "machine learning" is primarily focused on developing algorithms that enable computers to learn independently from data and past experience. Machine learning allows machines to automatically learn from data and predict outcomes without the need for explicit programming. Machine learning algorithms use historical sample data, known as "training data," to create mathematical models that facilitate automated predictions and decisions. Machine learning and statistics are used to create predictive models. Machine learning develops or uses its own algorithms. Providing more detail improves performance.

Predictive models are used in machine learning systems to predict outcomes in the face of new data. The accuracy of the predictions depends on the number of data sets used. With larger data sets, it is easier to create models that predict outcomes with greater accuracy.

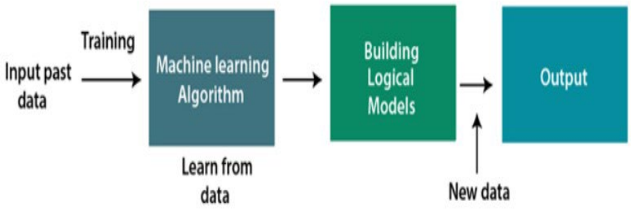

Figure 3. Processing of the Machine-Learning

Machine-Learning Features:

- Machine- learning uses facts to find pattern in data sets and automatically learns by learning from the past.
- Machine learning is information-driven technology.
- Data mining is similar to machine learning in that it uses large amounts of data.

Machine-learning requirements:

Machine learning is becoming more and more important. It can do things that are too hard for humans to do on their own. We need computer systems because we can't access so much data by hand. Machine learning can help us do this by teaching algorithms how to analyse data, make models, and automatically predict the output. We can provide them with huge amounts of data, and the cost function can tell us how well a machine learning algorithm will do compared to how much data we have. Machine learning can save us a lot of time and money.

Importance of the Machine Learning:

- Increasing data generation quickly
- Resolving challenging human-solvable situations
- Decisions are made in a wide range of areas, including financial matters.
- Analyzing data to uncover hidden patterns and draw out pertinent information.

Classification of Machine Learning

Categorized Machine learning into three types:

- Supervised
- Unsupervised
- Reinforcement

Classification of Machine Learning
Supervised Learning
Reinforcement Learning
Unsupervised Learning

Figure 4. Classification types of Machine Learning

Supervised Learning

This learning is a variety of machine-learning where a data-tagged, example-based training material is used to generate predictions of outcomes. To gain insight into each dataset, supervised learning systems use the labeled data as building blocks to construct models. After training and processing, models are evaluated against the sample data to determine whether they can accurately predict the desired outcome. A key objective of supervised learning lies in the mapping of input and output information. Supervision, similar to that of a student learning under the guidance of a teacher, is the foundation of supervised learning. Spam filtering one effective applications of supervised learning.

Two groups of algorithms may be used to further categories supervised learning:

- **Classification**
- **Regression**

Unsupervised Learning

It is a sort of instruction in which a computer is instructed without any supervision from a person. It all comes down to how the machine responds to the training data. Rearranging the data into new features or groupings of stuff with connected patterns is the aim. Unsupervised learning has no predetermined result; instead, the computer just searches through the enormous quantity of data it is provided in search of something valuable. Unsupervised learning is used by two primary categories of algorithms:

- **Clustering**
- **Association**

Reinforcement Learning

In reinforcement learning, learning agents get rewarded for every good thing they do and punished for every bad thing they do. These comments make it easier for them to learn automatically and get better at what they do. When an agent is learning, they look at their environment and interact with it. Their goal is to get as many reward points as possible, so their performance will get better. An example of this is a robot dog that can move its arms by itself.

Support Vector Machine Algorithm

Support Vector Machines (SVM's) are a common technique for addressing classification and regression issues. It is used to determine the most efficient approach to categorise the area so that fresh data points may be categorised fast. The support vectors and points that make up the optimum decision boundary, also known as the hyperplane, are included here. Look at the picture below. It is useful to divide decision boundaries and hyperplanes into two groups.

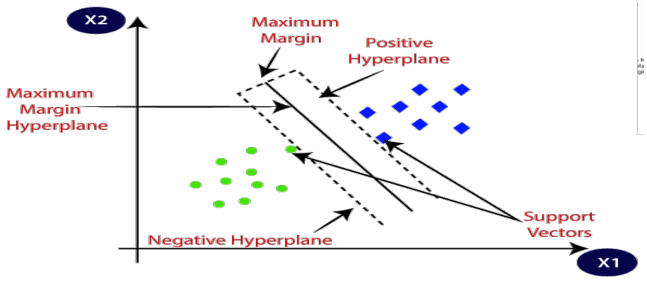

Figure 5. Representation of Support Vector Machine

Types of SVM

There are two kinds of support vector machines (SVM): linear SVM and non-linear SVM. Linear SVM is when data can be divided into two groups with just one directly line. That's what we call it. We use a classifier to classify this data. Non-linear SVM is when a dataset can't be classified with a straight line, so we use a classifier for that.

Hyper plane and Support Vectors in the SVM algorithm:

Hyper plane:

There may be several lines or decision boundaries that may be used to split classes in an n-dimensional space. But in order to categorise the data points, we must select the optimum decision boundary. The SVM hyperplane is the name of this ideal limit. The dimension of the hyperplane is dictated by the attributes of the data collection. For instance, the hyperplane will be a straight line if there are just two features (as in the example). So if there are 3 characteristics, the hyperplane is just 2D. SVM always creates a hyperplane with maximum margin and Maximum separation between data points.

Support Vectors:

A support vector is defined as the data point (or vector) that is closest to the hyperplane and has the greatest influence on the hyperplane's position. Therefore, support vectors are called support vectors because they are hyperplane supports.

What is Fuzzy Logic?

An unclear or ambiguous circumstance or remark is referred to as "fuzzy" in this context. In practise, it's possible that we can't always tell if something is true or untrue. For now, this notion offers a wide range of values between true and false, enabling you to choose the best answer to your problem.

Characteristics of Fuzzy Logic:

These are some of the traits of fuzzy logic:

- This idea is adaptable and simple to learn and put into practice.
- It is employed to assist in the reduction of human-created logics.
- It is the ideal way for figuring out answers to issues that can be resolved with approximation or uncertainty.
- It always provides two numbers, which stand for the two potential answers to a given issue or statement.
- It enables users to construct or develop non-linear functions of any complexity.
- Everything in fuzzy logic is a question of degree.
- Any logical system may be quickly fuzzified using fuzzy logic.
- It uses natural language processing as its foundation.
- Quantitative analysts utilize it as well to enhance the performance of their algorithms.
- It enables users to get in on the programming.

Fuzzy Logic System of Architecture:

Each element plays a significant part in the Fuzzy Logic system's architecture. The architecture is made up of the various four elements listed below:

- Rule Base
- Fuzzification
- Inference Engine
- Defuzzification

The following chart illustrates the structure or workflow of the Fuzzy logic system:

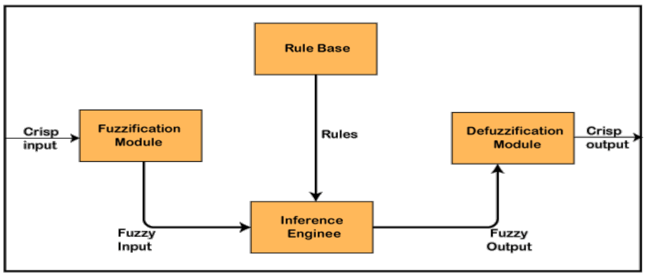

Figure 6. Fuzzy logic system Process

Rule Base:

The decision-making is governed by the If-Then conditions of the experts, and Rule Base holds the collection of rules. Recently, the fuzzy theory has undergone several improvements that provide efficient techniques for constructing and fine-tuning fuzzy controllers. The quantity of fuzzy sets of rules is reduced by these upgrades or advances.

Fuzzification:

A module or component known as "fuzzification" transforms the system inputs, or in other words, it turns crisp numbers into fuzzy steps. The inputs that are detected by the sensors and subsequently fuzzified and sent to the control systems for additional processing are known as crisp numbers. In a fuzzy logic system, this factor splits the input signal by five types:

- Large Positive-(LP)
- Medium Positive-(MP)
- Small-(S)
- Medium Negative-(MN)
- Large negative-(LN)

Inference Engine

Inference engines play an important role in any fuzzy logic system and FLS, because they analyze all data. Users can measure correlations between rules and actual fuzzy inputs. Once the correlation is determined, the system chooses the rule to be valid on the input array. A control action is generated by combining the results of each rule execution.

Defuzzification

A module or component known as defuzzification converts the fuzzy set input produced by the conjecture engine into a brittle value. It comes towards the end of the fuzzy logic system's phase. The user will accept the crisp value as a type of value. There are several methods available for doing this, but the user must choose the most effective one to minimize mistakes.

Membership Function

The function symbolizes the fuzzy set chart and enables users to put the linguistic word into numerical form. Every component of x is map in between 0 and 1 using this graph. Indicator or characteristics function are other names for this function.

A fuzzy set (A) is a set of U and M, where U is the discourse world and M is the member function, taking values in the interval (0, 1). The discourse world U is also called Ω or X.

$$\tilde{A} = \left\{\left(X, \mu\,\tilde{A}\,(X)\right)\middle|\, x\ \in X\right\}$$

Theory of Classical Set	Theory of Fuzzy Set
The concept is all about sets with sharp boundaries.	This theory is about sets that don't have any sharp edges.
It's defined by 0 and 1	It's based on the idea that there's always some kind of uncertainty about where a set's boundary is.
so there's no doubt about where a set is.	
It's used a lot in designing digital systems.	It is mainly used for fuzzy controllers.

4. Problem Domain

The below are some solved questions culled from a number of papers:

a. Attack detection efficiency is low.
b. Precision is affected by feature placement.
c. Attacks against U2R and R2L are less accurate.
d. Use of different classifier algorithms on smaller datasets
e. False positives and false negatives are still a big issue.

5. Proposed Workflow Diagram

In a number of journals, scholars discuss different forms of IDS algorithms and techniques. However, on NSL-KDD datasets, a hybrid solution is proposed in this article, which combines both Support Vector Machine and Machine Learning algorithms.

The proposed work stated in below flowchart:

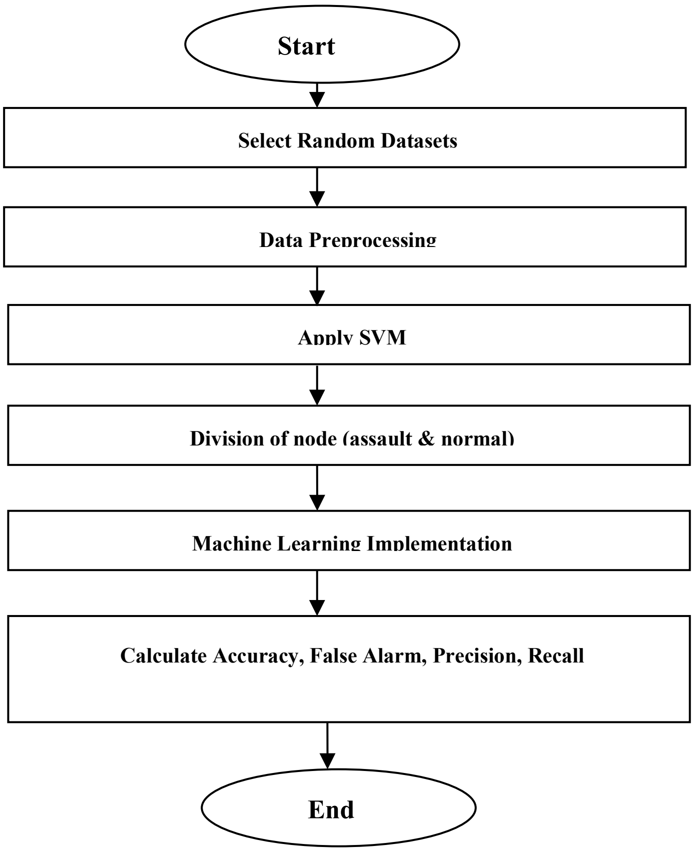
Start
Select Random Datasets
Data Preprocessing
Apply SVM
Division of node (assault & normal)
Machine Learning Implementation
Calculate Accuracy, False Alarm, Precision, Recall
End

Figure 7. Proposed Work Flowchart

My research suggests that the method should initially be run at random. Data preparation should be done once the data have been chosen from the dataset. The feature selection walkthrough and support are then executed. Finally, delete anything unnecessary or unused by using the vector engine. By classifying them as regular or attacks nodes, you can keep track of them. In the end, the data would be classified using machine learning techniques. Calculate the accuracy, false alarms, precision, and recall of your device.

6. Conclusion

An intrusion detection technique is a hardware or software program that looks for suspicious action on a network and alerts administrators. In this research, we explored different types of recognition systems and methods, including support vector machines and machine learning. I also looked into fuzzy logic and supervised learning. I compared different strategies for his KDD dataset based on their accuracy and after reviewing scientific papers, I also recommended his solution which is a hybrid of NSL dataset and his KDD dataset. After comparing the accuracy of different algorithms against different types of attacks, we came to the conclusion that intrusion detection protection is suitable not only for corporate users, but also for network users. In the future, we will work on improving the performance of various classifiers.

Acknowledgements.

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. The authors would like to thank the editor in chief, guest editors and anonymous reviewers for their comments that help improve the quality of this work.

References

[1] XIAOYAN WANG, HANWEN WANG. A High Performance Intrusion Detection Method Based on Combining Supervised and Unsupervised Learning. IEEE Smart World, Ubiquitous Intelligence & Computing Advanced & Trusted Computing, Scalable Computing, Internet of People and Smart City Innovations. 2018.

[2] MOHAMMAD EI BOUJNOUNI and MOHAMED JEDRA. New Intrusion Detection System Based on Support Vector Domain Description with Information Metric. International Journal of Network Security. 2018.

[3] KARUNA S.BHOSALE, Assoc. Prof. MARIA, Data Mining Based Advanced algorithm for intrusion detection in Communication Networks. International conference on Computational Techniques, Electronics & Mechanical System (CTEMS). 2018.

[4] P.AMALA, G. GAYATHRI, S.DINESH. Effective Intrusion Detection System Using Support Vector Machine Learning. International Journal of Advanced Science and Engineering Research. 2018.

[5] ELMER C. MATEL, ARIEL M.SISAN. Optimization of Network Intrusion Detection System using Genetic Algorithm with Improved Feature Selection Technique. Technological Institute of the Pilippines Quezon City, Phillipines. 2019.

[6] LUKMAN HAKIM, RAHILLA FATMA NOVRIANDI. Influence Analysis of Feature Selection to Network Intrusion Detection System Performance Using NSL-KDD Dataset. ICOMITEE 2019; October 16th-17th 2019; Jember, Indonesia in 2019.

[7] AFREEN BHUMGARA, ANAND PITALE. Detection of Network Intrusions Using Hybrid Intelligent System. International Conferences on Advances in Information Technology . 2019.

[8] RITUMBHRA UIKEY, Dr. MANARI CYANCHANDANI. Survey on Classification Techniques Applied to Intrusion Detection System and its Comparative Analysis. 4th International Conference on Communication and Electronics System (ICCES 2019) IEEE Conference Record #45898; IEEE Xplore ISBN; 978-1-7281-1261-9 . 2019.

[9] T.SREE KALA, A.CHRISTY, An Intrusion Detection System Using Opposition Based Particle Swarm Optimization Algorithm and PNN. International conference on Machine Learning, Big Data, Cloud and Parallel Computing, India 14th-16th feb 2019.

[10] KUNAL SINGH, Dr. K.JAMES MATHAI. Performance Comparison of Intrusion Detection System between DBN and SPELM Algorithm. National Institute of Technical Teacher Training $ Research, Bhopal India in 2019.

[11] ZHIYOU ZHANG, PEISHANG PAN. A Hybrid Intrusion Detection Method Based on Improved Fuzzy C-Means and SVM. International Conference on Communication Information System and Computer Engineer [CISCE] in 2019.

[12] Ghosh, H., Tusher, M.A., Rahat, I.S., Khasim, S., Mohanty, S.N. (2023). Water Quality Assessment Through Predictive Machine Learning. In: Intelligent Computing and Networking. IC-ICN 2023. Lecture Notes in Networks and Systems, vol 699. Springer, Singapore. https://doi.org/10.1007/978-981-99-3177-4_6

[13] Rahat IS, Ghosh H, Shaik K, Khasim S, Rajaram G. Unraveling the Heterogeneity of Lower-Grade Gliomas: Deep Learning-Assisted Flair Segmentation and Genomic Analysis of Brain MR Images. EAI Endorsed Trans Perv Health Tech [Internet]. 2023 Sep. 29 [cited 2023 Oct. 2];9. https://doi.org/10.4108/eetpht.9.4016

[14] Ghosh H, Rahat IS, Shaik K, Khasim S, Yesubabu M. Potato Leaf Disease Recognition and Prediction using Convolutional Neural Networks. EAI Endorsed Scal Inf Syst [Internet]. 2023 Sep. 21 https://doi.org/10.4108/eetsis.3937

[15] Mandava, S. R. Vinta, H. Ghosh, and I. S. Rahat, "An All-Inclusive Machine Learning and Deep Learning Method for Forecasting Cardiovascular Disease in Bangladeshi Population", EAI Endorsed Trans Perv Health Tech, vol. 9, Oct. 2023. https://doi.org/10.4108/eetpht.9.4052

[16] Mandava, M.; Vinta, S. R.; Ghosh, H.; Rahat, I. S. Identification and Categorization of Yellow Rust Infection in Wheat through Deep Learning Techniques. EAI Endorsed Trans IoT 2023, 10. https://doi.org/10.4108/eetiot.4603

[17] Khasim, I. S. Rahat, H. Ghosh, K. Shaik, and S. K. Panda, "Using Deep Learning and Machine Learning: Real-Time Discernment and Diagnostics of Rice-Leaf Diseases in Bangladesh", EAI Endorsed Trans IoT, vol. 10, Dec. 2023 https://doi.org/10.4108/eetiot.4579

[18] Khasim, H. Ghosh, I. S. Rahat, K. Shaik, and M. Yesubabu, "Deciphering Microorganisms through Intelligent Image

Recognition: Machine Learning and Deep Learning Approaches, Challenges, and Advancements", EAI Endorsed Trans IoT, vol. 10, Nov. 2023. https://doi.org/10.4108/eetiot.4484

[19] Mohanty, S.N.; Ghosh, H.; Rahat, I.S.; Reddy, C.V.R. Advanced Deep Learning Models for Corn Leaf Disease Classification: A Field Study in Bangladesh. Eng. Proc. 2023, 59, 69. https://doi.org/10.3390/engproc2023059069

[20] Alenezi, F.; Armghan, A.; Mohanty, S.N.; Jhaveri, R.H.; Tiwari, P. Block-Greedy and CNN Based Underwater Image Dehazing for Novel Depth Estimation and Optimal Ambient Light. Water 2021, 13, 3470. https://doi.org/10.3390/w13233470

[21] ZAKARIA EI MRABET. A Performance Comparison of Data Mining Algorithms Based Intrusion Detection System for Smart Grid. National Institute of Posts and Telecommunication Rabat, Morocco in 2019

[22] ADITYA PHADKE, MOHIT KULKARNI, PRANAV BHAWALKAR AND RASHMI BHATTAD . A Review of Machine Learning Methodologies for Network Intrusion Detection. 3rd National Conference on Computing Methodologies and Communication (ICCMC 2019) IEEE Xplore Part Number: cfp19k25-art; isbn; 978-1-5386-7807-4 in 2019.

[23] S.SIVANTHAM, R.ABIRAMI, R.GOWSALYA. Comparing the Performance of Adaptive Boosted Classifiers in Anomaly Based Intrusion Detection System for Networks. at International Conference on Vision towards Emerging Trends in Communication and Networking (ViTECoN) in 2019.

[24] RAJESH THOMAS, DEEPA PAVITHRAN . A Survey of Intrusion Detection Models Based on NSL-KDD Data Sets. 5th HCT INFORMATION TECHNOLOGY TRENDS (ITT 2018), Dubai, UAE, Nov, 2018.

[25] HASSAN AZWAR, MUHMMAD MURTAZ, MEHWISH SIDDIQUIE, SAAD REHMAN. Intrusion Detection in Secure Network for Cyber security Systems Using Machine Learning and Data Mining. IEEE 5th International Conference on Engineering Technologies & Applied Sciences, 22-23 Nov 2018, Bangkok Thailand in 2018.

[26] AZAR ABID SALIH, MAIWAN BAHJAT ABDULRAZAQ. Combining Best Features Selection Using Three Classifiers in Intrusion Detection System. International Conference on Advanced Science and Engineering (ICOASE), University of Zakho, Duhok Polytechnic University, Kurdistan Region, Iraq in 2019.

[27] Dr. UMA KUMARI, UMA SONI. A Review of Intrusion Detection using Anomaly Based Detection. 2nd International Conference on Communication and Electronics Systems (ICCES 2017) IEEE Xplore Compliant – Part Number: CFP17AWO-ART,ISBN:978-1-5090-5013- 0 IN 2017.