International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Analytics of Binary Class Detection & Forecasting of Cyber Incident by Machine Learning Methods

Swati Gawand[1*], Dr. Meesala Sudhir Kumar[2]

Submitted: 18/01/2024 **Revised**: 27/02/2024 **Accepted**: 04/03/2024

Abstract: In the rapidly evolving landscape of the digital era, the importance of cybersecurity has become paramount. As technology continues to advance, organizations and individuals are becoming increasingly interconnected, relying on digital platforms for communication, commerce, and critical infrastructure. This interconnectedness, while facilitating unprecedented convenience and efficiency, also exposes systems to a myriad of cybersecurity threats. This paper presents a proposed system designed to analyze network intrusion datasets. The dataset utilized comprises binary classified data, distinguishing between normal and attack types. We obtained the dataset from Kaggle for implementation purposes. Different machine learning methods, GNB, KNN, LR, SVM, DT, VC, RF, GB and XG are employed for the identification and categorization of cyber incident. A comparative analysis is conducted utilizing these machine learning algorithms. System performance is evaluated using Cross-Validation score, Recall value, F1 Score, Precision value and Accuracy value metrics. The analysis of system performance demonstrates which algorithm achieves the most accurate results.

Keywords: *Cyber Attack, Decision Tree, Logistic Regression, Random Forest.*

1. Introduction

Cybersecurity stands as the cornerstone of our modern digital age, offering a shield against the ever-looming threats of cyber incidents and data breaches. Its importance cannot be overstated, as it safeguards sensitive information, personal privacy, and critical infrastructure. In an era where digital transactions, communications, and interactions dominate our daily lives, cybersecurity ensures the integrity, confidentiality, and availability of data and systems. Moreover, cybersecurity fosters trust and confidence in digital technologies, enabling innovation, economic growth, and societal progress. Without robust cybersecurity measures in place, individuals, organizations, and governments face significant risks. As we navigate the complexities of our interconnected world, investing in cybersecurity is not merely an option but an imperative to safeguard our digital future and uphold the principles of privacy, security, and trust.

Cyber incidents come in various forms, each presenting unique challenges and threats to individuals, organizations, and society at large. Malware attacks, such as viruses, worms, and ransom ware, infiltrate systems to disrupt operations, steal sensitive information, or extort money. Phishing scams trick unsuspecting users into revealing personal information or login credentials through deceptive emails or websites. Denial-of-service (DoS) attacks involve overwhelming networks or websites with an excessive amount of traffic, effectively blocking access for genuine users. Meanwhile, Man-in-the-middle (MitM) attacks intercept and alter communications between parties, jeopardizing the confidentiality and integrity of data transmissions.. Data breaches expose sensitive information, such as financial records or personal data, due to unauthorized access or disclosure. Advanced persistent threats (APTs) involve sophisticated, long-term attacks aimed at infiltrating networks and extracting valuable data or intelligence. Each type of cyber incident underscores the critical need for robust cybersecurity measures, proactive risk management strategies, and ongoing vigilance to protect against evolving threats in the digital landscape.

This paper focuses on the task of analyzing a data to distinguish and forecast if it fits into the normal category or deviates as an anomaly. Our goal is to identify anomalies using various machine learning techniques. The dataset comprises two distinct categories of cyber incidents: genuine category and anonymous. We conduct a thorough examination of multiple machine learning methods on the provided dataset. Furthermore, we perform a comparative evaluation of the outcomes produced by each algorithm to ascertain the accuracy of our predictions. The objective of proposed work is to categorize instances as either secure or insecure communication, utilizing the attributes provided in the dataset. Each record is labeled as belonging to either the anomaly or normal class, contingent upon the features extracted.

1. To investigate whether feature selection consistently influences the prediction outcomes.

[1] Research Scholar, [2]Professor Department of Computer Science and Engineering, Sandip University, Mahiravani, Nashik 422213, Maharashtra, India.
[*]Corresponding author
swatigawand@gmail.com, sudhir.meesala@sandipuniversity.edu.in

2. To validate the effectiveness of various algorithm groups in accurately classifying anomalies.

3. To evaluate the resilience of the algorithms and determine the most appropriate algorithm for the objective.

Comparative examinations also uncover the performance disparities of each method with feature selection. In our evaluation of the algorithms, we consider metrics such as system performance i.e. accuracy, Precision reflects the accuracy of positive predictions among all positive instances, indicating the proportion of correctly identified positive cases out of all cases predicted as positive. Recall, on the other hand, measures the completeness of positive predictions, representing the proportion of correctly identified positive cases out of all actual positive cases, The F1 Score is a metric that balances both precision and recall, providing a single measure of a model's performance that considers both false positives and false negatives. Cross-Validation score evaluates the generalization ability of the model by assessing its performance on unseen data, achieved through techniques like k-fold cross-validation. This study focused on analyzing publicly available datasets, particularly the Network Intrusion Dataset. The dataset is available for access on Kaggle.

This study offers several key contributions, outlined below:

1. It conducts experiments utilizing a range of algorithms for categorizing and identifying cyber incidents.

2. It performs comparative analysis to assess the effectiveness of each method.

The subsequent sections of the paper adhere to the following framework:

- Section II explores the literature review.

- Section III offers a comprehensive explanation of the proposed system approach.

- Section IV delineates the experimental research undertaken.

- Section V concludes the research study and suggests future avenues of work.

2. Literature Review

In modern times, digitization and the internet have profoundly altered human lifestyles, enabling extensive social and commercial connectivity. However, cybercriminals exploit these platforms, leveraging systems to illicitly access private data. In mitigating this threat, cybersecurity professionals in the IT industry play an essential role. S. Sandosh et al. [13] proposed a model aimed at achieving high accuracy with minimal complexity and rapidity.

Preparation phase is conducted to remove null values, Refine the dataset by eliminating inconsistencies, and any irregularities present in the data. and other irregularities from the data. After preprocessing, valuable insights are derived from the refined data using the suitable feature selection algorithm [5]. Ensemble methods are employed for classification as they yield highly confident decisions and enhance overall accuracy through collaboration. In the field of cybersecurity, navigating challenges can stem from the plethora of security features available, and the effectiveness of a learning-based security model might fluctuate depending on the significance of these features and the attributes of the data. While Sarker et al. [8] we have explored diverse machine learning methodologies and their relevance in the domain of cybersecurity. A comprehensive analysis is necessary to determine their suitability for the specific [3] propose a cloud-based computing infrastructure designed to detect Distributed Denial of Service (DDoS) attacks. Despite advancements, current systems still face challenges such as excessive complexity, time constraints, and increased prediction inaccuracy, despite efforts aimed at enhancing accuracy and reducing false positive rates. Several gaps require attention in the current cybersecurity landscape:

1. Discovery of latent or novel attack patterns within datasets, such as the emergence of ransomware, a significant threat in today's digital environment.
2. Addressing the increased incidence of incorrect positives (IP) and incorrect negatives (IN), as these errors directly impact the precision and reliability of predictive models..
3. Developing predictive capabilities to anticipate the types of attacks likely to occur in the future, enhancing proactive security measures.

4. Within this segment, we explore multiple authors' research findings on machine learning-based cyber-attack detection models. Additionally, we scrutinize the limitations of the research.

3. Methodology

This section offers a comprehensive elucidation of the system methodology. Figure 1 depicts the Proposed Model. Within this model, the dataset serves as the input, initiating subsequent operations. Diverse machine learning algorithms are employed for model training. The dataset comprises binary classification data, with two distinct classes: normal and anomaly. The framework involves the following key steps:

1. Selection of the dataset to be utilized.

2. Implementing data refinement techniques to address irrelevant data within the dataset and conduct data transformation. Feature extraction is utilized to identify the most pertinent attributes from the dataset, thus improving the accuracy and efficiency of the detection model.

3. Partitioning data into training subset and testing subsets. During this stage, the proposed model is constructed and trained.

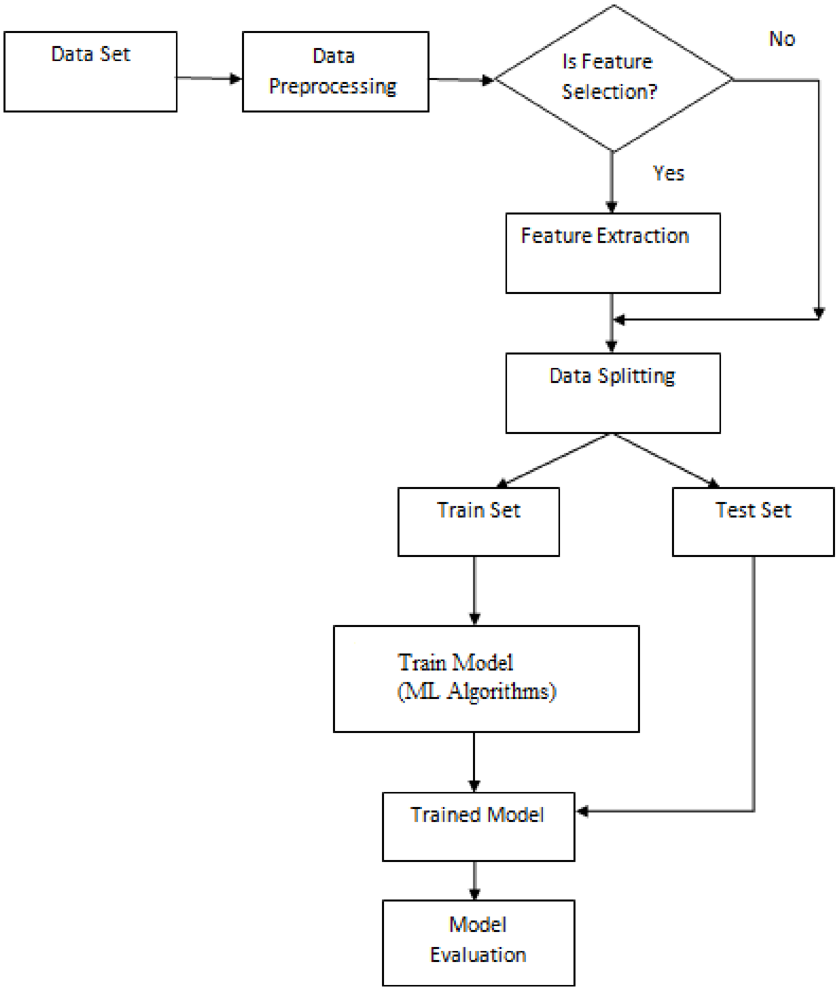

Fig 1 Proposed generic system

5. The model undergoes training utilizing a variety of machine learning methods/ algorithms. , including LR, GNB, SVM, DT ,VC, RF , KNN, GB, and XB.

6. The trained model undergoes evaluation with a test dataset, assessing its performance based on Cross-validation score (CV), F1 Score, precision, recall, training accuracy, and testing accuracy.

To train the model, we utilized a variety of machine learning methods.

1. Dataset

The experimental data was sourced from Kaggle [32], a publicly accessible data repository, containing a dataset representing a wide range of cyber intrusions, intended for identification purposes. Each data in the dataset is labeled as either normal class or anomalous class. On average, each connection data is 100 bytes long. The dataset consists of 42 columns and includes a total of 47,735 records.

The dataset utilized for implementation was obtained from Kaggle.

2 Data Preprocessing

During this phase, the rough data is prepped to be compatible with machine learning (ML) methods. We examine the dataset for any absent, null, or superfluous values, and then proceed to process the data to remove them from the dataset.

3 Extracting Features

Extracting Features involves identifying the most pertinent attributes from a dataset to build a model that improves detection accuracy and efficiency. Out of the dataset's 42 columns, a specific set of 10 features has been chosen intentionally for training. RFE (Recursive Feature Elimination) method systematically evaluates smaller subsets of features to identify the most relevant ones. Initially, the estimator is trained using the complete feature set. Then, less significant features are iteratively eliminated from the current set..

Splitting Data: - the data containing selective features are separated using the training –testing separation method. The grouping system reserves 30% of the dataset for testing and assign 70% for training, aimed at detecting attacks. After this partitioning, machine learning methods undergo training and evaluation using the specified training and testing datasets.

4. ML Methods

In this system, we employ the following machine learning algorithms: LR, GNB, SVM, DT ,VC, RF , KNN, GB, and XB.

1. Logistic Regression (LR):- It is a method used for grouping tasks, This is particularly relevant for predicting the result of a categorical dependent variable. It excels at forecasting categorical outcomes, ensuring clear and categorical conclusions. Logistic regression proves particularly effective when dealing with binary class labels [3].

2. Gaussian Naive Bayes (GNB):- This classification technique is utilized within Machine Learning (ML) frameworks, utilizing probabilistic principles . GNB functions under the premise that each parameter (commonly known as features or predictors) holds an independent predictive capability for the output variable. The model combines predictions from all parameters to produce a final prediction, providing the probability of the dependent variable being classified into each group.

3. Support Vector Machine (SVM):- The technique classifies data points that aren't linearly separable by projecting them into a high-dimensional feature space. This method identifies a boundary between the groups, transforming the data to facilitate the depiction of this boundary as a hyperplane.

4. Decision Tree (DT):- This algorithm assesses attributes at internal nodes, representing outcomes through branches, and stores class labels in leaf nodes. Its goal is to build a model using simple decision rules derived from data attributes to predict the value of a target variable. [30].

5. Voting Classifier (VC): - It consolidates predictions from each incorporated classifier, deciding the output class through a majority vote. Instead of constructing individual models and evaluating their accuracies independently, this method involves creating a single model that utilizes multiple classifiers, predicting outputs by aggregating their collective majority votes for each output [33].

6. Random Forest (RF):- This meta-estimator uses averaging To enhance predictive accuracy and reduce overfitting, the method involves training multiple decision tree classifiers on different subsets of the datase. [30].

7. K nearest Neighbour (KNN):- The method retains all available data and classifies new data points based on their similarity. Test data observations receive labels according to their proximity to the nearest neighbors within each class. Operating as a semi-supervised learning technique, KNN utilizes a nonparametric approach to classify samples. It computes distances between different points in the input vector, assigning unlabeled points to the nearest class, where "K" signifies the primary parameter in KNN classification. [3].

8. Gradient Boosting (GB):- This method enables the creation of a predictive model by amalgamating multiple weak prediction models, like decision trees..

9. XGBoosting (XB):- This is a highly advanced and scalable distributed gradient boosting library, crafted for efficiently training machine learning models. It employs an ensemble learning strategy, amalgamating predictions from multiple weak models to produce a more resilient prediction. Renowned for its ability to manage large datasets and achieve outstanding performance across various machine learning tasks, including classification and regression. [33].

3.5Trained Model: - here we input a testing dataset into the trained model and assess its performance using several metrics, including precision value, recall value, F1 Score, Cross-Validation (CV) Score, accuracy, training score, and testing scoreIn this proposed system, designed for binary class data, a variety of machine learning algorithms are utilized. We assess the performance of these algorithms and determine the one that attains the highest accuracy.

- **Data Analysis**

Throughout the experimental phase, the assessed outcomes comprised Precision value, Recall value, F1 Score, Cross Validation, Training value and Testing value. The experiments were conducted on a laptop running Windows 10 Enterprise 64-bit, equipped with an Intel(R) Core(TM) i3 CPU. The experimentation utilized the Python programming language.

Table 1 Assessment of Algorithm Performance

Name of Method	Precision Value	Recall Value	F1 Score	Accuracy Value
Logistic Regression	87	88	89	89
Gaussian Naive Bayes	86	85	86	85
Support Vector Machine	93	93	93	93
Decision Tree	96	96	96	96
Voting Classifier	92	91	90	90
Random Forest	95	96	96	95
K Nearest Neighbour	86	85	86	85
Gradient Boosting	83	82	82	81
XgBoosting	80	82	80	81

Table 1 showcases the performance outcomes of various machine learning methods. Random Forest (RF) achieves a score of 95% for Precision value, Recall value, and F1 Score, while Decision Tree (DT) achieves a s 96% score for each parameter. Likewise, regarding system performance, RF and DT both attain a score of 95% and 96%, respectively. Based on these findings, Based on the analysis, Based on the analysis, it can be concluded that Random Forest and Decision Tree algorithms yield more accurate results.

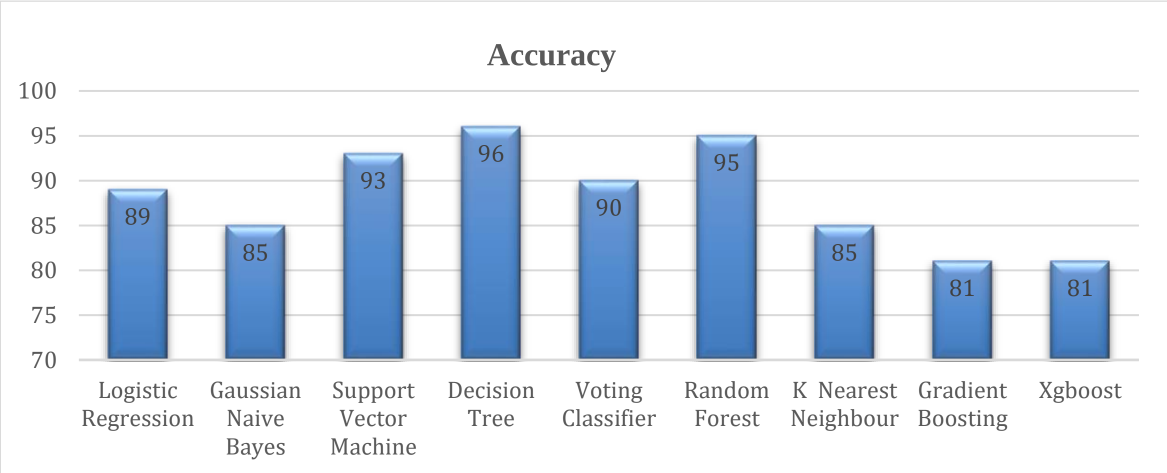

Fig 2 Comparison of Accuracy among Different Algorithms

Figure 2 depicts the accuracy of the proposed system. For the Accuracy parameter support vector machine Algorithms achieve 93% accuracy. Voting classifier achieve 90% accuracy. Random Forest achieves 95% accuracy, while Decision Tree achieves 96% accuracy.

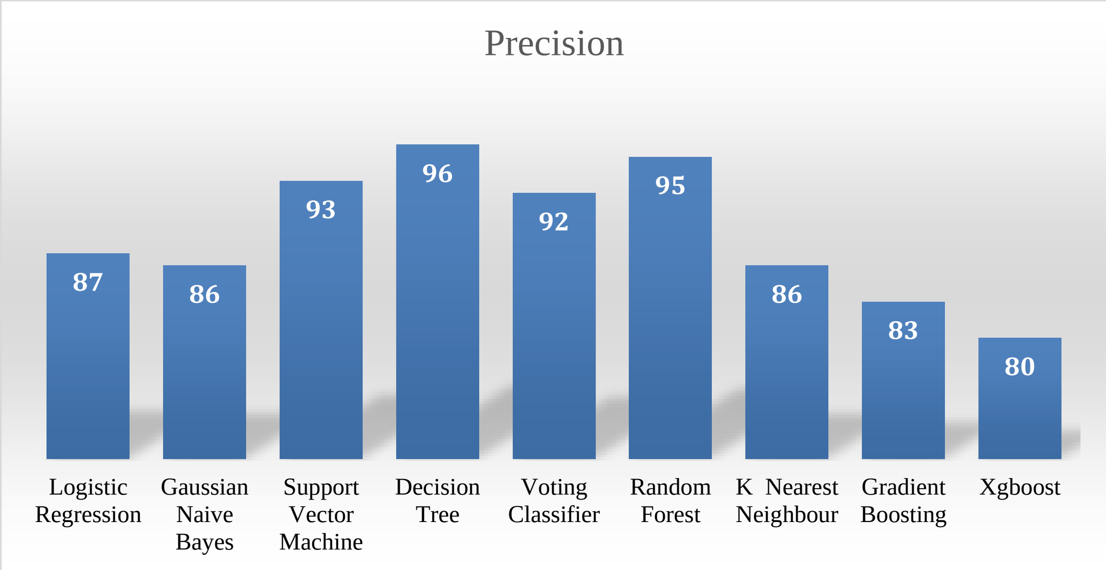

Fig 3 Precision Values Comparison across Various Algorithms

The provided Figure 3 illustrates a comparison of Precision values across different algorithms..

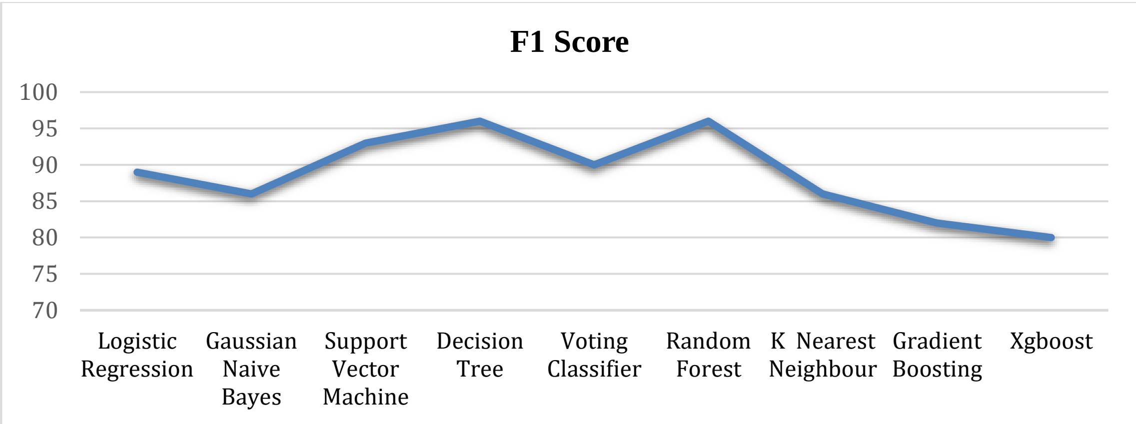

Fig 4 Contrast of F1 Score Metrics among Different Algorithms

Figure 4 displays a Contrast of F1 Score Metrics among Different Algorithms. It proves especially valuable when handling imbalanced datasets, where one class may outweigh the other significantly. Random Forest (RF) and Decision Tree (DT) attain a 96% F1 score, while Xgboost achieve a 90% F1 score.

Table 2 Evaluation of Performance: Training, Testing, and Cross-Validation Scores across Various Algorithms

Name of Method	Training Score	Testing Score	Cross Validation Score
Logistic Regression	76	72	76
Gaussian Naive Bayes	74	70	74
Support Vector Machine	81	79	82
Decision Tree	85	84	85
Voting Classifier	82	81	82
Random Forest	85	86	85
K Nearest Neighbour	70	68	68
Gradient Boosting	68	68	64
Xgboost	66	62	60

Table 2 Evaluation of Performance: Training, Testing, and Cross-Validation Scores across Various Algorithms. The training score of the Decision Tree (DT) algorithm is 85%. For Random Forest (RF) the train, test, and cross-validation scores are 85%. Based on these findings, it can be deduced that Random Forest and Decision Tree exhibit superior accuracy in classifying and predicting attacks.

5. Conclusion

Due to the rapid evolution of technology, ensuring system security has become increasingly challenging. Detecting cyber-attacks has become particularly daunting in today's landscape In this investigation, we have introduced a comparative Machine learning approach for detecting and predicting cyber-attacks. Our experimental analysis utilized a dataset containing two classes: Normal and Anomaly Upon examining the results, it was noted that the system achieved exceptional scores, reaching 95% with Decision Tree and Random Forest achieving 96%. Furthermore, support vector machine algorithms achieved a commendable accuracy of 93%.

The system is utilized for monitoring network security. In future research endeavors, our goal is to delve into multiclass datasets and evaluate the system's performance. Additionally, we intend to explore more intricate forms of cyber-attacks to bolster the system's capabilities further.

References

[1] Kousik Barik, Sanjay Misra, Karabi Konar, Luis Fernandez-Sanz & Murat Koyuncu," Cybersecurity Deep: Approaches, Attacks Dataset, and Comparative Study", Applied Artificial Intelligence, Published with license by Taylor & Francis Group, pp 1-25, DOI: 10.1080/08839514.2022.2055399,2022

[2] Blessing Guembe, Ambrose Azeta, Sanjay Misra, Victor Chukwudi Osamor, Luis Fernandez-Sanz & Vera Pospelova," The Emerging Threat of Ai-driven Cyber Attacks: A Review", Applied Artificial Intelligence, Published with license by Taylor & Francis Group,1-36, DOI: 10.1080/08839514.2022.2037254,2022

[3] Mona Alduailij, Qazi Waqas Khan, Muhammad Tahir, Muhammad Sardaraz, Mai Alduailij, and Fazila Malik," Machine-Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance Method", Cloud Computing and Symmetry: Latest Advances and Prospects,1-15, DOI https://doi.org/10.3390/sym14061095,2022

[4] Arpitha. B, Sharan. R, Brunda. B. M, Indrakumar. D. M, Ramesh, "Cyber Attack Detection and notifying System using ML Techniques", Indian Journal of Computer Science and Engineering (IJCSE), pp 28153-28159,2021

[5] Fahima Hossain, Marzana Akter and Mohammed Nasir Uddin," Cyber Attack Detection Model (CADM) Based on Machine Learning Approach ",2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), pp 567-572,2021

[6] Abdulkadir Bilen and Ahmet Bedri Özer," Cyber-attack method and perpetrator prediction using machine learning algorithms", PeerJ Computer Science, pp 475-496,2021

[7] Florian Klaus Kaiser, Tobias Budiga," Attack Forecast and Prediction ", C&ESAR'21: Computer Electronics Security Application Rendezvous, pp 77-97, 2021

[8] Iqbal H. Sarker, CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks, Internet of Things, Volume 14,2021,100393, ISSN 2542-6605,

[9] I. H. Sarker, Y. B. Abushark, F. Alsolami, A. I. Khan, Intrudtree: A machine learning based cyber security intrusion detection model, Symmetry 12 (5) (2020) 754.

[10] I. H. Sarker, A. Kayes, S. Badsha, H. Alqahtani, P. Watters, A. Ng, Cybersecurity data science: an overview from a machine learning perspective, Journal of Big Data 7 (1) (2020) 1–29.

[11] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, K. Sakurai, Machine learning-based iot-botnet attack detection with sequential architecture, Sensors 20 (16) (2020) 4372.

[12] A. Bansal and S. Kaur, "Data Dimensionality Reduction (DDR) Scheme for Intrusion Detection System Using Ensemble and Standalone Classifiers," In Proc. International Conference on Advances in Computing and Data Sciences, vol. 1045, pp. 436-451, 2019. doi 10.1007/978-981-13-9939-8 39 [Accessed 15 July 2020].

[13] S. Sandosh, V. Govindasamy, and G. Akila, "Enhanced intrusion detection system via agent clustering and classification based on outlier detection," Peer-to-Peer Networking and Applications, vol. 13, no. 3, pp. 1038-1045, 2020. doi: 10.1007/s12083-019-00822-3 [Accessed 15 July 2020

[14] R. Wazirali, "An Improved Intrusion Detection System Based on KNN Hyperparameter Tuning and Cross-Validation," Arabian Journal for Science and

Engineering, vol. 45, no. 12, pp. 10859-10873, 2020. doi 10.1007/s13369-020-04907-7 [Accessed 19 August 2020].

[15] Twinkle Shah, Sagar Parmar, Kishan Panchal," Cyber Crime Attack Prediction", International Research Journal of Engineering and Technology, pp 1037–1042. 2020

[16] Kumar, "Cyber-attack prediction using machine learning algorithms", International Conference on Advances in Computing, Communication and Control (ICAC3), pp 1–5,2020

[17] A. Ahmim, M. Ferrag, L. Maglaras, M. Derdour and H. Janicke, "A Detailed Analysis of Using Supervised Machine Learning for Intrusion Detection," Strategic Innovative Marketing and Tourism, pp. 629-639, 2020.

[18] W. Zong, Y. Chow, and W. Susilo, "Interactive three-dimensional visualization of network intrusion detection data for machine learning," Future Generation Computer Systems, vol. 102, pp. 292-306, 2020

[19] O. Sarumi, A. Adetunmbi, and F. Adetoye, "Discovering computer networks intrusion using data analytics and machine intelligence," Scientific African, vol. 9, p. p 1-5, 2020.

[20] A. Nagaraja, B. Uma, and R. Gunupudi, "UTTAMA: An Intrusion Detection System Based on Feature Clustering and Feature Transformation," Foundations of Science, vol. 25, no. 4, pp. 1049-1075,2020.

[21] A. Saleh, F. Talaat, and L. Labib, "A hybrid intrusion detection system (HIDS) based on prioritized k-nearest neighbors and optimized SVM classifiers", Artificial Intelligence Review, vol. 51, no. 3, pp. 403-443, 2020.

[22] H. Liu and A. Gegov, "Collaborative Decision Making by Ensemble Rule-Based Classification Systems," Studies in Big Data, pp. 245-264, 2020.

[23] P. Negandhi, Y. Trivedi and R. Mangrulkar, "Intrusion Detection System Using Random Forest on the NSL-KDD Dataset," Emerging Research in Computing, Information, Communication and Applications, pp. 519-531, 2019.

[24] C. Gayathri Harshitha, M. Kameswara Rao, and P. Neelesh Kumar, "A Novel Mechanism for Host-Based Intrusion Detection System," In Proc. , "First International Conference on Sustainable Technologies for Computational Intelligence, pp. 527-536, 2019.

[25] Y. Ever, B. Sekeroglu and K. Dimplier, "Classification Analysis of Intrusion Detection on NSL-KDD Using Machine Learning Algorithms," In Proc. International Conference on Mobile Web and Intelligent Information Systems, pp. 111-122, 2019.

[26] T. Tang, D. McLernon, L. Mhamdi, S. Zaidi and M. Ghogho, "Intrusion Detection in SDN-Based Networks: Deep Recurrent Neural Network Approach," Deep Learning Applications for Cyber Security, pp. 175-195, 2019.

[27] A. Gupta, G. Prasad and S. Nayak, "A New and Secure Intrusion Detecting System for Detection of Anomalies Within the Big Data," Studies in Big Data, pp. 177-190, 2018.

[28] M. Ibrahim, "An empirical comparison of random forest-based and other learning-to-rank algorithms, "Pattern Analysis and Applications, vol. 23, no. 3, pp. 1133-1155, 2019.

[29] M. G. Raman, N. Somu, S. Jagarapu, T. Manghnani, T. Selvam, K. Krithivasan, V. S. Sriram, An efficient intrusion detection technique based on support vector machine and improved binary gravitational search algorithm, Artificial Intelligence Review (2019) 1–32.

[30] Mahmudul Hasan, Md. Milon Islam, Md Ishrak Islam Zarif, M.M.A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches", Internet of Things, Volume 7,2019,100059, ISSN 2542-6605,https://doi.org/10.1016/j.iot.2019.100059.

[31] https://pub.towardsai.net/gaussian-naive-bayes-explained-and-hands-on-with-scikit-learn-4183b8cb0e4c

[32] https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection

[33] Sonia Wadhwa, Dr. Sudhir Kumar Meesala, "An Artificial System for Prognosis Cancer Cells through Blood Cells Images Using Image Processing", International Journal of Science and Research (IJSR), Volume 8 Issue 6, June 2019, pp. 638-642, https://www.ijsr.net/getabstract.php?paperid=ART20198513.

[34] Sudhir Kumar Meesala, Dr. Pabitra Mohan Khilar, Dr. A. K. Shrivastava, "Multiple Instruction Multiple Data (MIMD) Implementation on Clusters of Terminals", International Journal of Science and Research (IJSR), Volume 5 Issue 1, January 2016, pp. 1652-1658,

https://www.ijsr.net/getabstract.php?paperid=NOV153204.

[35] Meesala, Sudhir & Pabitra, Mohan & Khilar, & Shrivastava, Ajeet & Scholar, Ph. (2014). Multiple Instruction Multiple Data (MIMD) Implementation on Clusters of Terminals. 10.13140/RG.2.1.4826.9846.

[36] Mishra, Sudha & Chandra, Pankaj & Soni, Dr & Gupta, Akanksha & Tiger, Bindu & Kumar, Dr & Singh, Dr. (2023). TUMOR DETECTION AND COMPARATIVE ANALYSIS Section A-Research paper ISSN. 12. 148-172. 10.48047/ecb/2023.12.si13.115.

[37] Kumar, Meesala & Murugan, Chitra & Sharma, Anubhav & Ragavendiran, S & Banappagoudar, Sudharani & Kumar, A. (2023). RECOGNITION OF EMOTIONS THROUGH SPEECH USING MACHINE LEARNING TECHNIQUES. 26. 723-437.

[38] Munusamy, Ambigavathi & Sridharan, D. (2020). A Survey on Big Data in Healthcare Applications. 10.1007/978-981-13-8618-3_77.

[39] Gawand Swati, and Santosh Kumar. "Energy Efficient Clustering Method for Wireless Sensor Network by using Compressive Sensing and MEMAC." International journal of computer Applications 975 (2014): 8887.

[40] S. K. Meesala, "Parallel processing implementation on clusters of terminals using Java RMI," 2012 International Conference on Computing, Communication and Applications, Dindigul, India, 2012, pp. 1-6, doi: 10.1109/ICCCA.2012.6179167.