ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1128

A Robust Intrusion Detection System Empowered by Generative Adversarial Networks

Vijayaganth V.[1]; Dharshana M.G.[2]; Sureka P.[3]; Varuna Priya S.[4]
Assistant Professor (Sl.G)[1]
Department of Artificial Intelligence and Data Science, KPR Institute of Engineering and Technology[1,2,3,4]

Abstract:- There is a very bleak outlook on cyber security due to the rapid expansion of the Internet and the ever-changing terrain of cyber-attacks. This paper explores the field of intrusion detection through network analysis, with a particular emphasis on applying machine learning (ML) and deep learning (DL) approaches. For every ML/DL technique, a thorough tutorial overview is given together with a review of pertinent research publications. These studies were read, indexed, and summarised according to their thermal or temporal correlations with great care. The paper also provides information on frequently used network datasets in this field, which is relevant given the critical role that data plays in ML/DL techniques. It also discusses the difficulties in using ML/DL for cyber security and provides insightful recommendations for future lines of inquiry. Interestingly, the KDD data set shows up as a reputable industry standard for intrusion detection methods. A lot of work is being done to improve intrusion detection techniques, and both training and evaluating the detection model's quality depend equally on the quality of the data. The KDD data collection is thoroughly analysed in this research, with a special emphasis on four different attribute classes: Basic, Content, Traffic, and Host. We use the Modified Random Forest (MRF) technique to classify these properties.

Keywords:- *Intrusion Detection, Feature Selection, Machine Leaning.*

I. INTRODUCTION

The security of computer networks and data has become crucial in the current digital era. Strong network intrusion detection systems (NIDS) are essential now more than ever because of the complexity of cyber threats and the interconnectedness of our systems. By detecting illegal access and averting possible risks to information systems, intrusion detection plays a critical part in protecting enterprises. But conventional intrusion detection techniques frequently struggle to keep up with the dynamic threat landscape. In order to address these issues and improve intrusion detection efficacy, we suggest a novel method dubbed "Network Intrusion Detection with Two-Phased Hybrid Ensemble Learning and Automatic Feature Selection." The goal of this project is to integrate state-of-the-art methods from cybersecurity, data science, and machine learning. Our goal is to revolutionise network intrusion detection by fusing autonomous feature selection and the capabilities of ensemble learning into a two-phased detection method.

A. Feature Selection

The security of networks and information systems has become critical in today's ever-expanding digital world. The proliferation of cyber dangers, encompassing sophisticated malware and advanced persistent threats, underscores the need for network intrusion detection systems (NIDS) to be constantly evolving in order to thwart hostile actions and unauthorised access. NIDS effectiveness is largely dependent on the selection of the most pertinent data properties, or "features." In machine learning and data analysis, feature selection is a crucial step where the main goal is to find and keep valuable qualities while eliminating redundant or unnecessary ones. To increase the effectiveness and precision of the detection process in the context of network intrusion detection, careful feature selection is crucial.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1128

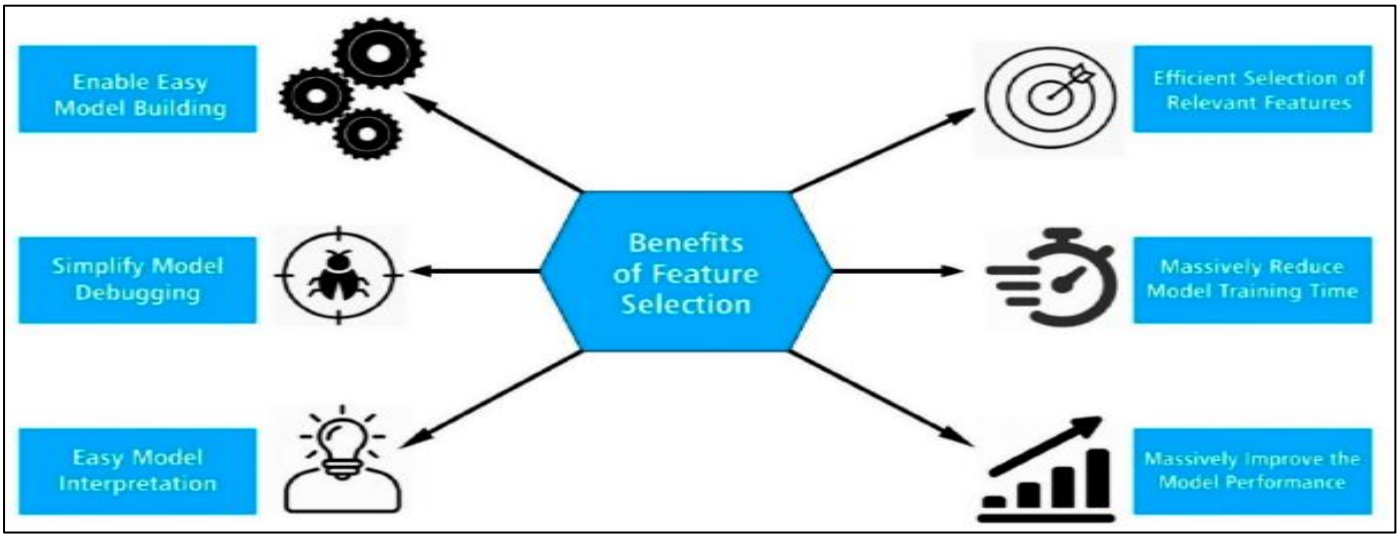

Fig 1: Feature Selection

II. LITERATURE REVIEW

In this research, Felix Obite [1]et al. suggest that the substantial increase in Internet traffic validates the transition of the backbone of the telecommunications industry from a time division multiplexing (TDM) orientation to an emphasis on Ethernet solutions. In a market historically dominated by DSL and cable modems, Ethernet PON, which combines inexpensive Ethernet and fibre infrastructures, has emerged as the leading technology. With the help of this innovative technology, which is easy to use, reasonably priced, and scalable, end customers can receive a vast array of data services across a single network. A summary of EPON's history is given in the paper, with an emphasis on the present work being done on next-generation high-data-rate access networks including NG-PON2, WDM PON, and OFDM PON. Furthermore, the recently finished 100G-EPON is reviewed to illustrate the most current developments in the sector. The document is to provide network operators and interested practitioners with the knowledge they need to plan and prioritise their actions by providing a thorough and current review. The study also attempts to find technological answers for additional research. Broadband services that are capable of supporting high-speed internet transmission are required due to the rise in data traffic and the increasing number of online users who spend more time online and use bandwidth-intensive apps. It is anticipated that this would help the economy grow. Therefore, in order to support these novel and real-time broadband applications, future access networks will need to have a lot of capacity and mobility.

The fifth generation (5G) of wireless broadband access, which is presently being deployed by Mobile Network Operators, has garnered considerable attention in recent years [2]. Surprisingly, though, not as much focus has been placed on "Wi-Fi 6," the latest IEEE 802.1ax standard in the family of wireless local area networks that is intended for private edge networks. The suitability of cellular and Wi-Fi technologies for providing high-speed wireless Internet connectivity is reviewed by Edward J. Oughtonet al. in this research. With the goal of supporting the Internet of Things and machine-to-machine communications, as well as providing faster wireless broadband connectivity, both cellular and Wi-Fi technologies seek to improve performance. These technologies can therefore be considered technical alternatives in a variety of use cases. The authors draw the conclusion that both technologies will be significant players in the future, acting as both competitors and allies at the same time. Due to its cheaper deployment costs, Wi-Fi 6 is expected to remain the favoured option for interior use, while 5G is expected to remain the preferred technology for wide-area coverage.

Somayye Hajiheidari [3] et al. has suggested a system that lowers the power consumption of electrical appliances, adding a new dimension to intelligent things. By integrating electronic devices and linking them to the Internet, this system enhances commonplace physical things and allows for communication with cyberspace and local intelligence. The network of connected things is referred to as the Internet of Things (IoT) in this notion. Nevertheless, because IoT items are directly connected to the Internet, malevolent people can attack them. These assaults, referred to as internal attacks, take advantage of IoT devices' resource limitations to compromise internal nodes and launch network attacks. Thus, it is impossible to exaggerate the significance of Intrusion Detection Systems (IDSs) in the Internet of Things. Notwithstanding its importance, there aren't many thorough and organised evaluations that address and examine the workings of IDSs in Internet of Things environments. This work proposes a Systematic Literature Review (SLR) of IDSs in the IoT to fill this vacuum. The article offers comprehensive classifications of intrusion detection systems (IDSs) according to their methodology (anomaly-based, signature-based, specification-based, and hybrid), architecture (centralised, distributed, hybrid), evaluation technique (simulation, theoretical), and attack types (denial of service, Sybil, replay, selective forwarding, wormhole, black hole, sinkhole, jamming, false data, attack).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1128

The ensemble of classifiers [4], often referred to as an ensemble learner, has attracted a lot of interest in the field of cybersecurity research, especially in the area of intrusion detection systems (IDSs). IDSs are essential for stopping cyberattacks, and creating a better detection framework is necessary to increase their detection capabilities, particularly when using ensemble learning. The choice of accessible base classifiers and combiner algorithms present two major issues in ensemble creation. This work uses a systematic mapping analysis to provide an overview of the use of ensemble learners in IDSs. A total of 124 well-known articles from the body of existing literature were gathered and analysed for the study. These papers were then categorised according to factors such as the datasets utilised, publication sites, years of publication, ensemble methodologies, and IDS techniques. Furthermore, an empirical research of a novel classifier ensemble approach for anomaly-based IDS dubbed stack of ensemble (SoE) is reported and analysed in the work. The SoE is an ensemble classifier that combines three distinct ensemble learners—random forest, gradient boosting machine, and extreme gradient boosting machine—in a homogenous way using a parallel architecture. The accuracy, false positive rates, area under the ROC curve metrics, and Matthews correlation coefficients of classification algorithms are statistically analysed to assess their performance. By offering a current comprehensive mapping analysis and a thorough empirical review of recent developments in ensemble learning techniques applied to IDSs, this work closes a gap in the literature.

As a result of recent developments in mobile technology, the ubiquitous use of IoT-enabled gadgets in our daily lives has created security challenges. Muhamad Erza Amina [5] et al. have provided a solution that overcomes these issues. The primary cause for concern is that open wireless networks, including Wi-Fi, are susceptible to impersonation assaults. In these attacks, the adversary poses as an authorised participant in a communications protocol or system. Due to the widespread use of linked devices, massive amounts of high-dimensional data are generated, which complicates simultaneous detections. To address this issue, the paper suggests a brand-new strategy known as Deep-Feature Extraction and Selection (D-FES). Weighted feature selection and stacked feature extraction are combined in D-FES. Reconstructing pertinent information from unprocessed inputs yields meaningful representations through the application of layered auto encoding. Subsequently, a shallow-structured machine learner-inspired modified weighted feature selection is integrated with this. Experimental results on the Aegean Wi-Fi Intrusion Dataset (AWID), a well-referenced Wi-Fi network benchmark dataset, show the efficacy of the proposed D-FES. The findings demonstrate an impressive 99.918% detection accuracy and a 0.012% false alert rate. These results demonstrate that the suggested D-FES is the most precise technique for identifying impersonation assaults that has been documented in the literature. Furthermore, the reduced feature set obtained from D-FES minimises computational cost while simultaneously lessening the bias of machine learning models.

III. RELATED WORK

The increasing number and diversity of network threats means that traditional firewalls and data encryption methods are no longer adequate to fulfil the expectations of modern network security. Thus, intrusion detection systems have been proposed to handle network threats. The current mainstream intrusion detection methods still suffer from low detection rates and a significant feature engineering overhead, despite the assistance of machine learning. In order to address the issue of low detection accuracy, this research suggests a deep learning model for network intrusion detection (DLNID). It accomplishes this by fusing an attention mechanism with a bidirectional long short-term memory (Bi-LSTM) network. Initially, a convolutional neural network (CNN) network is used to extract sequence features of data traffic; subsequently, the attention mechanism is used to reassign the weights of each channel; and lastly, Bi-LSTM is used to learn the network of sequence features. Significant data imbalances are often present in public intrusion detection data sets. In order to solve issues with data imbalance, this paper creates a generally symmetric dataset by extending minority class sample sizes through the use of adaptive synthetic sampling, or ADASYN. Moreover, information fusion is enhanced by reducing data dimensionality through the use of a modified stacked auto encoder.

IV. METHODOLOGY

The suggested network intrusion detection system (IDS) uses the MODIFIED RANDOM FOREST (MRF) algorithm to categorise network traffic as either malicious or legitimate. The method divides the KDD dataset's data properties into four groups: Basic, Content, Traffic, and Host. An MRF classifier is then trained on each group. The monitored network's network traffic data is gathered by the system, which then pre-processes it to extract pertinent features before feeding the features into the MRF classifiers. Every data point generates a prediction from the classifiers, and the system uses the average prediction to generate the final forecast. Inspired by negative selection-based detection generation, the suggested methodology is tested on the NSL-KDD dataset, which is an altered version of the popular KDD CUP 99 dataset. Additionally, by automatically choosing parameter values based on the training dataset utilised, the system becomes more flexible and adaptive.

A. Probability Model

In this module, we preprocess the training data for the probability model that is used to capture a user's typical mentioning behaviour. In a social network stream, we describe a post by its number of mentions, called ask, and the set V of user names (IDs) that are referenced in it. In this case, two kinds of infinity need to be taken into account. The first kind, called ask, deals with the quantity of users that are referenced in a post. We try not to impose an artificial restriction on the number of cited users, even if it is impracticable for a user to mention hundreds of other users in a single post. Rather, to remove any inherent limitation, we use a geometric distribution and integrate out the

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1128

parameter. The number of users who may be named is the subject of the second kind of infinite. We use the Chinese Restaurant Process (CRP), which is well-known for its application in handling infinite vocabularies, for estimating in order to avoid limiting the amount of potential references.

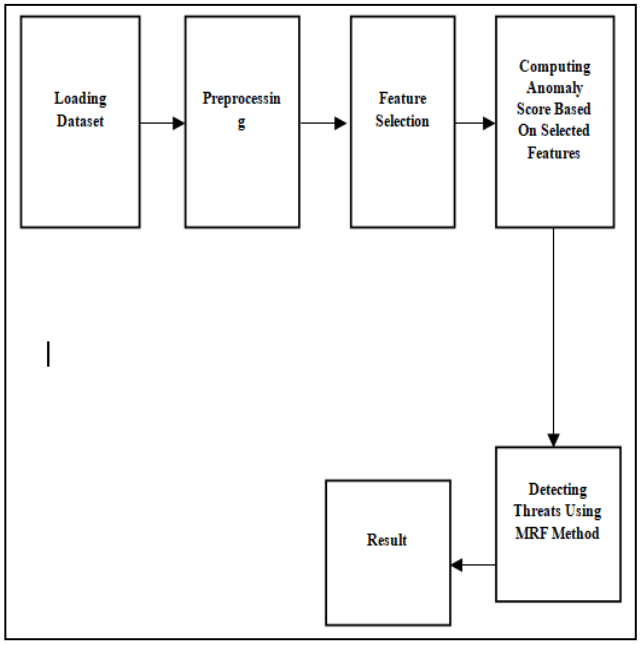

Fig 2: Block Diagram

B. Computing the Link-Anomaly Score

We introduce a mechanism in this module to compute the divergence of a user's behaviour from the modelled normal mentioning behaviour. We compute the likelihood using the training set T(t)u to find the anomaly score of a new post by user u at time t, which includes k mentions to users V. The posts published by user u within the time period [t-T, t], where T is set to 30 days in this project, comprise the training set T(t)u. This computation is then used to define the link-anomaly score. The predictive distribution of the number of mentions and the predictive distribution of the users who are mentioned can be used to calculate the two terms in the equation given above.

C. Change Point Analysis and DTO

This approach is a development of the suggested Change Finder technique, which uses new data compressibility to detect changes in a time series' statistical dependence structure. This module uses MRF coding, also known as Modified Random Forest (NML) coding, as a coding criterion in place of the plug-in predictive distribution. Two tiers of scoring procedures are involved in the identification of a change point. Change points are detected by the second layer, whilst outliers are identified by the first. The scoring criterion for each layer is determined by calculating the prediction loss for an autoregressive (AR) model using the MRF coding distribution. While determining the ideal NML code length is challenging, the suggested SNML offers a sequentially computed approximation. Discounting is also used by the MRF while training the AR models. Lastly, a threshold is applied in our method to turn the change-point scores into binary alarms.

D. Modified Random Forest Detection Method

We covered change-point detection based on MRF and DTO in the earlier parts. We have tested our approach in conjunction with Kleinberg's Modified Random Forest detection method in this module. Specifically, we have put into practice Kleinberg's Modified Random Forest detection approach in two states. Since a non-hierarchical structure is anticipated in this experiment, the two-state variant was selected. A probabilistic automata model with two states—the Modified Random Forest state and the non-Modified Random Forest state—serves as the foundation for the Modified Random Forest detection technique. It is assumed that some events, like posts arriving, occur in accordance with a time-varying Poisson process, the rate parameter of which is dependent on the state at any given moment.

V. ALGORITHM DETAILS

Machine Learning (ML) and Deep Learning (DL) approaches are used, with a particular emphasis on the Modified Random Forest (MRF) approach, to analyze the KDD dataset.

Intrusion Detection with Modified Random Forest

➢ *Step 1: Data Pre-processing*

- Load the KDD dataset
- Pre-process the data, handle missing values, encode categorical features, etc.

➢ *Step 2: Feature Engineering*

- Extract relevant features from the dataset
- Optionally, perform dimensionality reduction techniques

➢ *Step 3: Split the Dataset*

- Split the dataset into training and testing sets

➢ *Step 4: Modified Random Forest (MRF) Training*

- Initialize the MRF model with hyper parameters
- Train the MRF model using the training set

➢ *Step 5: Model Evaluation*

- Use the trained MRF model to make predictions on the testing set
- Evaluate the model's performance using Detection Rate (DR) and False Alarm Rate (FAR)

➢ *Step 6: Attribute Analysis*

- Analyze the contributions of each attribute class (Basic, Content, Traffic, Host) to DR and FAR
- Optimize the dataset by adjusting features to achieve maximum DR while minimizing FAR

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1128

VI. RESULT ANALYSIS

Results from the empirical analysis of the KDD dataset using the Modified Random Forest (MRF) technique are instructive for the Intrusion Detection Systems (IDS) industry. By dividing the dataset into four categories—Basic, Content, Traffic, and Host—the study illustrates the distinct contributions of each attribute class to the Detection Rate (DR) and False Alarm Rate (FAR). By reducing false alarm rate (FAR), which stops unnecessary false alerts, and increasing detection ratio (DR), which is a measure of successful intrusion detection, the dataset may be optimised by this thorough study. The findings demonstrate the critical role attribute class considerations play in the development of trustworthy intrusion detection models and provide useful data for enhancing the efficacy of cyber security protocols.

Table 1: Comparison Table

Algorithm	Accuracy
NB, and DT	75
MRF	88

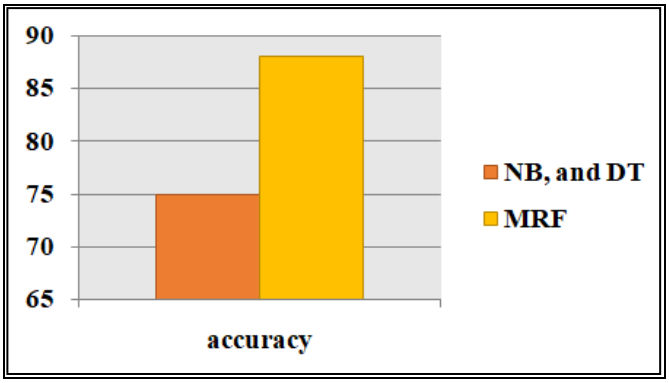

Fig 3: Comparison Graph

The table shows the accuracy outcomes of several algorithms, such as Modified Random Forest (MRF), Decision Trees (DT), and Naive Bayes (NB), within the framework of a specific inquiry. Fascinatingly, the Modified Random Forest (MRF) scores 88%, far higher than the combined accuracy of 75% achieved by Naive Bayes and Decision Trees. These accuracy metrics indicate the MRF algorithm's effectiveness in the context under study by showing how well it performs in comparison to its NB and DT competitors. The MRF algorithm is displayed in the table as a potential choice for the current task, emphasising how important algorithm selection is to achieving higher accuracy rates.

VII. CONCLUSION

In summary, a network intrusion detection system (IDS) that employs a modified random forest (MRF) algorithm exhibits potential for precisely identifying network intrusions while resolving concerns related to overfitting, adaptability, flexibility, and resilience against new threats. MRF-based intrusion detection systems are easy to install and train, and they are capable of efficiently monitoring sizable networks. These systems are able to detect a wide range of network threats, such as malware, port scanning, and denial-of-service attacks. It is imperative to recognise that no intrusion detection system is perfect. Like other IDS systems, MRF-based systems are vulnerable to evasion strategies. Furthermore, MRF-based IDS systems can be computationally demanding to train and run.

FUTURE WORK

MRF classifiers are well known for their remarkable accuracy in classification tasks; however, there is room for improvement. Later research could focus on developing new MRF algorithms with improved precision and performance. Hackers are always coming up with new ways to get around IDS systems. Subsequent efforts can focus on creating MRF classifiers that are more resistant to these evasion strategies. Training and operation can involve significant computing costs. Subsequent investigations may focus on developing novel training algorithms and optimisation strategies that can reduce the computing load of MRF classifiers.

REFERENCES

[1]. The research "An intellectual intrusion detection system using hybrid hunger games search and remora optimisation algorithm for IoT wireless networks" was carried out by R. Kumar, A. Malik, and V. Ranga. It was published in the journal Knowledge-Based Systems in November 2022.

[2]. W. Wang, S. Jian, Y. Tan, Q. Wu, and C. Huang created a representation-learning-based network intrusion detection system that records explicit and implicit feature interactions. In January 2022, the journal Computer Security published their research.

[3]. W. Lehr, J. Oughton, K. Katsaros, I. Selinis, D. Bubley, and J. Kusuma investigated the differences between Wi-Fi 6 and 5G wireless internet access possibilities [3]. In June 2021, the journal Telecommunication Policy published their findings.

[4]. A cross-benchmark evaluation and systematic mapping study on ensemble learning for intrusion detection systems was carried out by B. A. Tama and S. Lim. In February 2021, the journal Computer Science Review published their research.

[5]. S. Lei, C. Xia, Z. Li, X. Li, and T. Wang developed a novel model dubbed HNN for analysing temporal-spatial analysis and multi-feature correlation as the foundation for intrusion detection in [5]. October 2021 saw the publication of their findings in the IEEE Transactions on Network Science and Engineering.

[6]. Y. Cheng, Y. Xu, H. Zhong, and Y. Liu, "Leveraging semisupervised hierarchical stacking temporal convolutional network for anomaly detection in IoT communication," IEEE Internet Things Journal, volume 8, issue 1, January 2021, pages 144–155.

[7]. In July/August 2021, IEEE Trans. Dependable Secure Comput., vol. 18, no. 4, pp. 1591–1604, "Sustainable ensemble learning driving intrusion detection model," Z. Ma, C. Zhong, Y. Xiang, X. Li, M. Zhu, L. T. Yang, M. Xu, and H. Li

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR1128

[8]. Developing an efficient feature selection and ensemble classifier-based intrusion detection system, Computer Networks, vol. 174, June 2020, Article no. 107247; Y. Zhou, G. Cheng, S. Jiang, and M. Dai.
[9]. "MLEsIDSs: Machine learning-based ensembles for intrusion detection systems—A review," written by M. R. Ayyagari, G. Kumar, and K. Thakur November 2020; Journal of Supercomput., 76, no. 11, pp. 8938-8971.
[10]. Reference 10 A. Tama, B. A., L. Nkenyereye, S. M. R. Islam, and K. Kwak, "An enhanced anomaly detection in web traffic using a stack of classifier ensemble," IEEE Access, vol. 8, pp. 24120–24134, 2020.