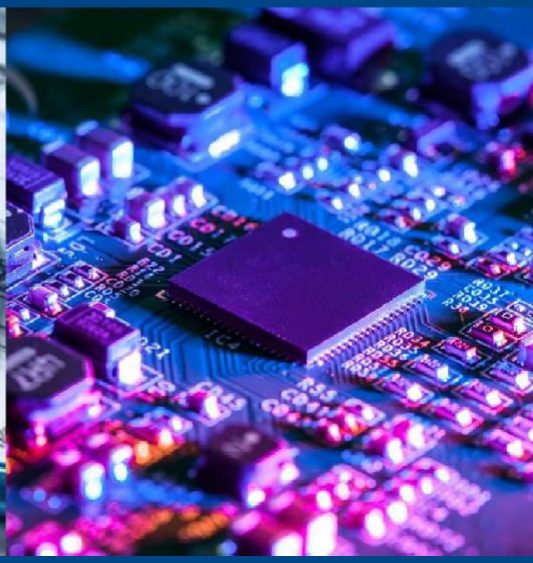
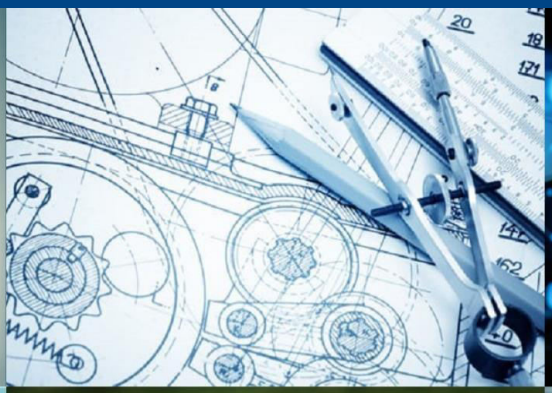
ISSN: 2582-7219

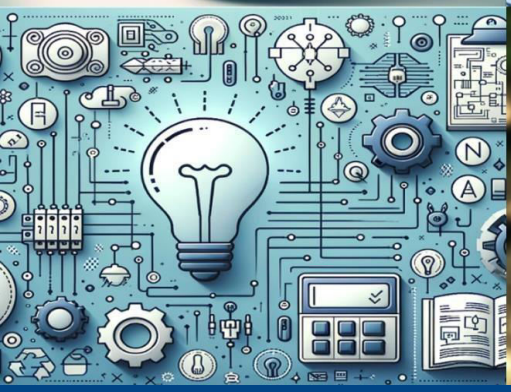




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 8, August 2025

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808018

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A Hybrid Model Approach for Intrusion Detection System Based on Machine Learning

Praveen A G, Sravanthi K

Dept. of MCA, AMC Engineering College, Bengaluru, India

Assistant Professor, Dept. of MCA, AMC Engineering College, Bengaluru, India

ABSTRACT: The cybersecurity threat landscape is being greatly expanded by the exponential growth of data and the quickening pace of digitization. When used with firewalls, intrusion detection systems (IDS) greatly enhance network security. Traditional intrusion detection systems, on the other hand, are statically designed, which leaves them open to obsolescence and necessitates costly retraining programs. Since dynamic models can learn from incoming traffic without depending on prior data or incurring significant retraining costs, they are effective at handling continuous streams of network traffic, which has expanded their necessity. In light of this challenge, we have implemented a more effective approach: an Intrusion Detection System (IDS) that uses incremental majority voting to enhance the robustness and adaptability of intrusion detection. This system makes use of existing tools and procedures. With a specific emphasis on reducing false alarm rates, our system aims to improve the efficacy and precision of real-time intrusion detection by combining the decision-making powers of multiple machine learning models, such as the KNN classifier, the Softmax Regressor, and the Adaptive Random Forest classifier. The results of this research show that for the most common attacks, the model achieves a precision of 100% and an accuracy of 96.43%. Our constructed model has great potential as an effective solution for Intrusion Detection Systems (IDS) and can handle real-world imbalanced datasets well. It successfully handles the unbalanced properties of streaming data.

I. INTRODUCTION:

New forms of cyberattacks like as distributed denial of service (DDoS), ransomware, and advanced persistent threats (APTs) are appearing at an alarming rate, making intrusion detection a must- have in today's cybersecurity landscape. In order to effectively prevent potential attacks and safeguard the integrity of the network, security systems need robust components. To protect systems from hostile activity and prevent unauthorized access, Intrusion Detection Systems (IDS) are becoming crucial tools.

In order to tackle these challenges with network security, there has been a lot of study in the field of intrusion detection that uses machine learning and deep learning techniques. Despite the fact that these studies have been successful in classifying different forms of attack, they face two major obstacles. The majority of intrusion detection systems (IDS) in use today are static and cannot learn or adapt in real- time. This necessitates costly retraining processes and limits their effectiveness in identifying newly emerging attacks. Secondly, it may be challenging and expensive to get the large, well labelled datasets that are generally necessary for these supervised models. Large datasets could also have significant storage requirements. All the more reason to develop intrusion detection approaches that are both flexible and economical with resources, so we can deal with new threats as they emerge without having to waste a ton of time or space on labels. To tackle the problem of idea drift in intrusion detection, our method is derived from the CDIL (circular dilated convolution) network, which used a mixed incremental model with majority voting. But our study yielded better results in terms of performance. Additionally, our technique shows promise as a valuable tool for real-world cybersecurity applications by effectively responding to emerging threats while maintaining high detection accuracy over time.

II. LITERATURE REVIEW

Gustavo De Carvalho Bertoli; Lourenço Alves Pereira Júnior; Osamu Saotome; Aldri L. Dos Santos; Filipe Alves Neto Verri; Cesar Augusto Cavalheiro Marcondes; Sidnei Barbieri; Moises S. Rodrigues; José M. Parente De Oliveira, An End-to-End Framework for Machine Learning- Based Network Intrusion Detection System, 2021, Network intrusion detection systems have challenges from design to

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

implementation due to the proliferation of connected devices and attackers' evolving strategies. Therefore, network intrusion detection systems apply machine learning constantly. However, these studies employ old background and assault traffic data. To guarantee complete solution implementation, this paper describes the AB-TRAP architecture, which uses existing network traffic and addresses operational difficulties. The five steps of AB-TRAP include creating the attack dataset, authentic dataset, machine learning model training, model installation, and model performance evaluation. We used the AB-TRAP to detect TCP port scanning attacks on the LAN and internet. A decision tree with minimal kernel CPU and RAM utilization yielded an F1- score of 0.96 and an area under the ROC curve of 0.99 in the LAN case study. Eight machine learning approaches gave the internet instance an average F1- score of 0.95, an average area under the ROC curve of 0.98, and 1.4% CPU and 3.6% RAM overhead in user space on a single-board computer. This framework is repeatable, uses the newest network traffic, attacks, and manages model implementation and deployment issues.

Ngan Tran; Haihua Chen; Jay Bhuyan; Junhua Ding, Data Curation and Quality Evaluation for Machine Learning-Based Cyber Intrusion Detection, 2022, Intrusion detection is essential for cyber security. Many studies have proposed sophisticated methods for detecting intrusions using large datasets, however they have ignored the importance of data quality. Poor data quality includes mislabeled, erroneous, incomplete, irrelevant, inconsistent, duplicated, and overlapping data. We tested eight machine learning models and two pre-trained language models, BERT and GPT- 2, on 11 host-based intrusion datasets to see how data quality affects machine learning performance. We found that BERT and GPT-2 outperformed all other models in every dataset. Pre-trained models performed differently from typical machine learning approaches when data duplications and overlaps occurred. Pre-trained models were less susceptible to duplicate and overlapping data than typical machine learning models. Eliminating overlaps and duplicates from training data using a predefined sequence similarity range may improve pre-trained models on most datasets. However, it may hurt model performance in datasets with comparable sequences. Duplicates in test data may undermine model evaluation. The overlap rate between the normal and intrusion classes seems to be inversely related to pre-trained model intrusion detection performance. From the results, we developed a model selection and data quality verification approach for a high-quality machine learning-based intrusion detection system.

Machine Learning and Deep Learning Approaches for CyberSecurity: A Review Asmaa Halbouni; Teddy Surya Gunawan; Mohamed Hadi Habaebi, 2022**,** The rapid innovation and expansion of the internet over recent decades have heightened concerns over the escalating and evolving nature of cyber-attacks. Consequently, an efficient intrusion detection system was necessary to safeguard data, and the emergence of artificial intelligence's sub-disciplines, machine learning and deep learning, represented one of the most effective solutions to this issue. This article examined intrusion detection systems and analyzed the sorts of learning methods used by machine learning and deep learning to safeguard data from harmful activities. It examines contemporary advancements in machine learning and deep learning, including diverse network implementations, applications, algorithms, learning methodologies, and datasets to create an operational intrusion detection system.

P. L. S. Jayalaxmi; Rahul Saha; Gulshan Kumar; Mauro Conti; Tai-Hoon Kim, Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey, 2022, The rising prevalence of connected devices in the Internet of Things (IoT) age has correspondingly heightened the incidence of intrusions. An Intrusion Detection System (IDS) is a supplementary intelligent system designed to monitor, identify, and alarm about hostile activity; an Intrusion Prevention System (IPS) is an advanced extension of a detection system that initiates appropriate action upon suspicion of an attack. Both Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are essential and beneficial for formulating a security framework. Numerous research examine detection and prevention models; yet, there is a lack of consistency in the opportunistic improvements of these models. Moreover, the current models include some limitations that need examination to formulate new security models. This survey is the inaugural research to conduct risk factor analysis using mapping techniques and to provide a hybrid framework for an effective security model for intrusion detection and/or prevention. We examine the significance of several Artificial Intelligence (AI) approaches, tools, and methodologies used for detection and prevention systems in the Internet of Things (IoT). We concentrate on Machine Learning (ML) and Deep Learning (DL) approaches for intrusion detection and prevention systems, offering a comparative study that highlights feasibility, compatibility, limitations, and real-time concerns. This study is advantageous for both business and academics in identifying the obstacles and concerns within existing security models and in developing new dimensions of security frameworks using efficient machine learning or deep learning approaches.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Li Zou; Xuemei Luo; Yan Zhang; Xiao Yang, HC-DTTSVM: A Network Intrusion Detection Method Based on Decision Tree Twin Support Vector Machine and Hierarchical Clustering, 2023, Network intrusion detection is a key technology in national cybersecurity strategy and has become a hot topic in cybersecurity research. Effective and efficient intelligent network intrusion detection utilizing advanced machine learning algorithms is essential for defending complex networks from varied network assaults. HC- DTTWSVM, which combines decision tree twin support vector machine with hierarchical clustering, detects different network intrusions. The hierarchical clustering technique is used to build the network traffic data decision tree, using a bottom-up merging approach to separate the higher nodes and reduce error accumulation. The created decision tree executes the network intrusion detection model using twin support vector machines, allowing top-
down category identification. The HC-DTTWSVM technique is tested using the NSL-KDD and UNSW- NB15 intrusion detection benchmark datasets. HC- DTTWSVM can detect different network intrusions and performs similarly to other methods, according to experiments.

Machine Learning for Misuse-Based Network Intrusion Detection: Overview, Unified Evaluation and Feature Choice Comparison Framework, Laurens Le Jeune; Toon Goedemé; Nele Mentens, 2021, Protecting complex communication networks requires network intrusion detection technologies. These systems originally recognized signs, trends, and rule violators, but today artificial intelligence and machine learning algorithms provide exciting alternatives. However, the literature uses outdated datasets and several evaluation metrics to prove algorithm efficacy. For worldwide comparability, this study consolidates algorithms across settings and includes two new evaluation criteria. Large-scale comparisons are possible with the detection and identification scores' trustworthy evaluation of a network intrusion detection system's performance. Additionally, we provide a method for converting raw packet flows into machine learning input characteristics. This platform quickly runs many algorithms on multiple datasets and allows systematic performance comparisons. Our experiments match and surpass the state-of-the-art, proving this method's potential. Raw traffic input characteristics are easier and cheaper to extract, making them suitable for real- time deep learning systems.

Treepop Wisanwanichthan; Mason Thammawichai, A Double-Layered Hybrid Approach for Network Intrusion Detection System Using Combined Naive Bayes and SVM, 2021, Many basic network intrusion detection systems employ signature-based pattern matching. For abnormality and unique threat detection, a machine learning classifier works better. One machine learning classifier cannot recognize all attack types, especially unusual ones like Remote2Local (R2L) and User2Root (U2R), due to large assault pattern variances. A hybrid approach has higher performance potential. This study proposes a Double-Layered Hybrid Approach (DLHA) to address the problem. We used Principal Component Analysis (PCA) variables to maximize variance for each attack type and found that R2L and U2R attacks behave like typical users. DLHA uses Naive Bayes classifiers to recognize DoS and Probe attacks and SVM to distinguish R2L and U2R from ordinary situations. Our study was compared to other published research utilizing the NSL-KDD data set. The experiments show that DLHA outperforms numerous modern IDS methods and any machine learning classifier. At 96.67% for R2L and 97% for U2R, DLHA detects uncommon attacks well.

Seyed Mohammad Hadi Mirsadeghi; Hayretdin Bahsi, Learning From Few Cyber-Attacks: Addressing the Class Imbalance Problem in Machine Learning-Based Intrusion Detection in Software-Defined Networking, 2023, Learning algorithms perform poorly on minority classes, which may pose greater dangers than majority classes, due to class imbalance. This article compares balancing and unbalanced learning strategies for SDN intrusion data. The academic community has solved the imbalance problem in machine learning-based intrusion detection, but SDN is novel and effective. To further SDN intrusion detection research, InSDN, the sole publicly available SDN intrusion detection dataset, must address the class imbalance problem. We solve class imbalance utilizing data- and classifier-level methods. Our research aims to find ways to mitigate class imbalance in machine learning-based intrusion detection in SDN. We propose GAN-Siamese Neural Network deep learning architectures for generative modeling and similarity-driven intrusion detection. This research compares classification benchmarks utilizing ROS, SMOTE, GANs, weighted Random Forest, and Siamese-based one- shot learning. We found that Random Forest (RF) classifies minority class instances better than deep learning models. This supports Random Forest's class imbalance management. ROS and SMOTE, common balancing approaches, lower the False Positive Rate (FPR) and increase the FNR when categorizing minority populations. In conclusion, data-level techniques improve classification performance over deep learning models but decrease RF performance, leading to more inaccurate predictions. Therefore, RF needs no further balancing to improve performance. This research addresses class imbalance in SDN intrusion data and provides a well-structured benchmark for any network intrusion detection data. Therefore, it may greatly impact future study in this subject.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Taehoon Kim; Wooguil Pak , Early Detection of Network Intrusions Using a GAN-Based One- Class Classifier, 2022, Network security requires timely intrusion detection. However, most network intrusion detection system research uses features from full sessions, making it difficult to detect intrusions before a session ends. The suggested method uses packet data to identify malicious transmissions. This method increases the risk of misidentifying regular packets as intrusions or intrusions as normal traffic during the first session. To distinguish network intrusions from benign sessions, the presented method detects problematic packet patterns. A new Generative Adversarial Network (GAN) training dataset is created utilizing misclassified data from the previous training dataset, which the LSTM-DNN model utilized. The GAN trained on this dataset can determine whether the LSTM-DNN can classify the current packet. If the GAN cannot identify the packet, the detection phase is aborted and repeated with the next packet. The painstaking classification technique, which includes LSTM-DNN and a GAN validation model, detects network intrusions in real time without session termination or packet collecting delays. Numerous studies demonstrate that the recommended strategy may detect intrusions before session termination while maintaining detection effectiveness equivalent to existing methods.

Yue Li; Jiale Zhang; Yiting Yan, Enhancing Network Intrusion Detection Through the Application of the Dung Beetle Optimized Fusion Model, 2023, Due to fast advances in information communication and mobile device technology, smart devices have become popular, making homes easier and life smarter. This movement promotes innovation in healthcare, transportation, and business. As technology advances, network security issues have grown, making data and digital life security critical. Network security has always required intrusion detection. Network traffic anomaly detection is the main method used by conventional intrusion detection systems to detect intrusions. Modern intrusion detection relies on machine learning-based algorithms to identify unusual activities and potential intrusions by analyzing network traffic patterns. To overcome these issues, this study introduces a new intrusion detection model that combines the Attention-CNN- BiLSTM (ACBL) and Temporal Convolutional Network (TCN) architecture The ACBL and TCN models analyze network traffic data geographically and temporally well. Multiple neural network designs improve model performance and accuracy in this integration. The Tent mapping-enhanced Dung Beetle Optimization Algorithm (TDBO) optimizes feature selection parameters and searches for model hyperparameters based on dung beetle behavior. The TDBO feature selection parameters are combined with the Random Forest relevance ranking to help choose the best features for model performance. The TDBO-ACBLT intrusion detection model is introduced and tested using the UNSW-NW15 dataset. Harris's Hawk Optimization (HHO), Particle Swarm Optimization (PSO), and Dung Beetle Optimization (DBO) are less accurate than TDBO in feature selection and parameter optimization. The recommended strategy outperforms machine learning approaches in accuracy.

III. PROBLEM STATEMENT

When it comes to identifying and preventing malicious activities, wireless networks face serious threats from the security of the Internet of Things (IoT). In order to detect such intrusion attempts or attacks, it is crucial to quickly and accurately identify any suspicious or unlawful network activity. Differentiating between safe and harmful network activity requires an advanced intrusion detection system (IDS). In dynamic, resource-limited wireless networks, the effectiveness of Intrusion Detection Systems (IDS) is critical for rapid detection and intervention. It is necessary to use specialized detection and mitigation strategies for various threats, including as flooding, injection, and impersonation attacks. In order to better protect wireless networks from sophisticated assaults, this research aims to improve intrusion detection system technology. Our aim is to navigate the complexities of wireless network security and pave the way for future Intrusion Detection System capability upgrades, so we can better protect ourselves from the ever-changing cybersecurity landscape.

IV. METHODOLOGY

The main objective of this research is to develop an effective intrusion detection system with a low false positive rate using ensemble learning techniques. In this study, we present a classifier composed of three machine learning classifiers selected from different families. The choice of classifiers is motivated by the ‘‘no free lunch’’ theorem, aiming to leverage models that complement each other during the classification process.

The study focuses on enhancing network security through an Intrusion Detection System (IDS) using a hybrid model approach. This research is applicable in cybersecurity domains, including:

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

1. **Network Security & Cyber Threat Detection** – Identifying malicious activities in network traffic.
2. **Machine Learning in Cybersecurity** – Utilizing AI-based models for anomaly and signature-based intrusion detection.
3. **Ensemble Learning for IDS** – Improving detection rates through a voting classifier that integrates multiple machine learning models.
4. **Benchmark Datasets** – The study employs standard datasets like **NSL-KDD, CICIDS2017, or UNSW- NB15** for model training and evaluation.
5. **Real-World Applications** – The research applies to enterprise security, cloud computing, and IoT environments where robust intrusion detection is critical.

1. Data Collection

- Utilize publicly available intrusion detection datasets (**NSL-KDD, CICIDS2017, UNSW-NB15**) containing labeled network traffic data (normal & attack instances).
- Preprocess the data by handling missing values, normalizing features, and encoding categorical variables.

2. Feature Selection & Engineering

- Apply feature selection techniques like **Principal Component Analysis (PCA), Recursive Feature Elimination (RFE), or Mutual Information Gain** to optimize model efficiency.
- Extract key network traffic attributes, such as packet size, protocol type, duration, and connection status.

3. Hybrid Model (Voting Classifier) Development

- Implement multiple machine learning models, such as:
  - **Decision Trees (DT)** – Interpretable model for classifying attacks.
  - **Random Forest (RF)** – Reduces overfitting and enhances robustness.
  - **Support Vector Machine (SVM)** – Effective in handling high-dimensional data.
  - **K-Nearest Neighbors (KNN)** – Useful for pattern recognition.
  - **Artificial Neural Networks (ANN)** – Captures complex data relationships.
- Use **Voting Classifier (Soft & Hard Voting)** to combine predictions and improve classification performance.

4. Model Training & Evaluation

- Split data into **training (80%) and testing (20%) sets** using **Stratified K-Fold Cross-Validation** to prevent bias.
- Train individual classifiers and integrate them into the **Voting Classifier**.
- Evaluate performance using metrics:
  - **Accuracy, Precision, Recall, F1-Score, AUC- ROC**
  - **False Positive Rate (FPR) and False Negative Rate (FNR)**

5. Performance Comparison & Optimization

- Compare the hybrid model's performance with individual classifiers.
- Tune hyperparameters using **Grid Search or Bayesian Optimization**.
- Test the model in a simulated **real-time intrusion detection scenario**.

Proposed System Design:

A comprehensive overview of the suggested system is shown in Figure 1 below. In the past, several methods were created to detect the kind of suspicious activity or intrusions mentioned in [15] and [6]. Unfortunately, problems such as a high rate of false alarms and poor classification accuracy continue to plague these systems. The primary function of the system is to get data from the associated Twitter account by means of the Twitter API and to include the most recent comments that have been seen on Twitter. Most importantly, social media networks do not have enough software to detect suspicious or malicious accounts. To address the challenges posed by modern computer systems, our research combined natural language processing (NLP) with machine learning (ML) techniques. In order to gather information, we first examine several social networking websites. Both the original data sources and the files containing the datasets get it. Due to its gathering from several web sources, including Twitter, the data may sometimes be in an unstructured form. Essential data pre-processing steps include data filtering and a targeted sample strategy. A combination of the bloom filter and systematic sampling was used to separate the data. To remove instances that were wrongly classified, the bloom filter was used. In order to make phrase identification and tokenization easier, electrical analysis is required.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A string array is the best place to store tokenized words since it makes string verification much easier. Several ML and deep learning methods were used to classify the whole network. Many ML techniques, such as recurrent neural networks, were part of this strategy. During runtime, the proposed method may detect potentially dangerous objects.

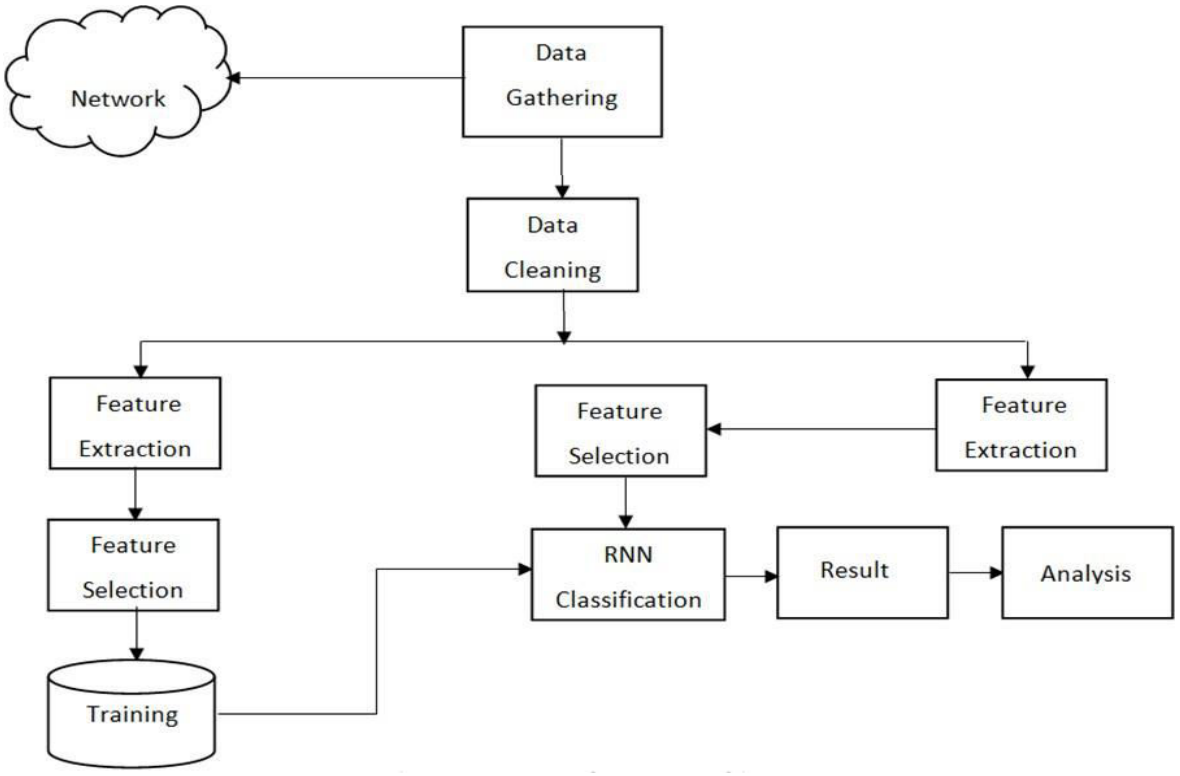
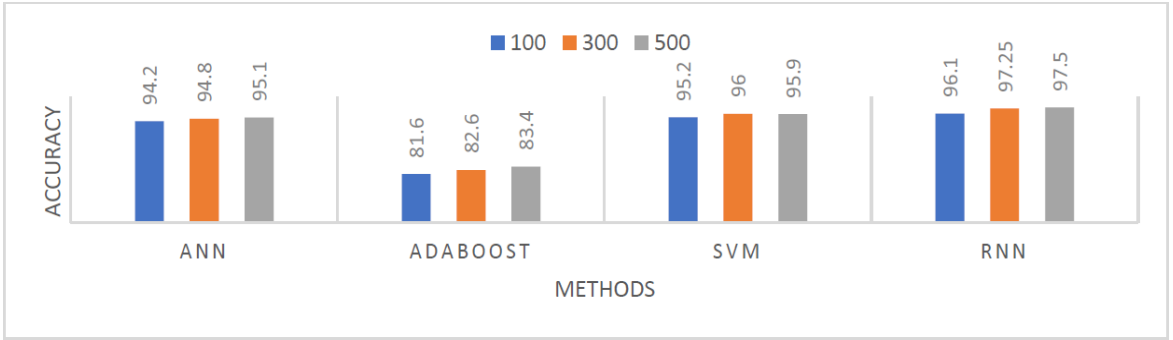


Fig. 1: System architecture for IDS using machine learning technique

V. RESULTS AND DISCUSSION

All other algorithms evaluated in a separate study using the same evaluation measures were outperformed by our suggested RNN algorithm in terms of prediction effectiveness. Additionally, not all datasets are representative of software problems and new flaws to the same extent due to limitations in data quantity and quality. The proposed solution may be subjected to further testing if it is integrated into live software systems. The three-split data approach allows for ten-, fifteen-, or twenty-fold cross-validation.

Using the same or comparable datasets, the system compares the findings of this study to four other systems. A comparison of traditional and modern machine learning (ML) approaches is shown in Figure 2.



ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Fig. 2: Comparative analysis of proposed vs existing classification for attack detection

Figure 2 compares the performance of two top machine learning algorithms for threat identification with the proposed techniques. This graphic shows how the proposed RNN outperforms machine learning methods in terms of accuracy.

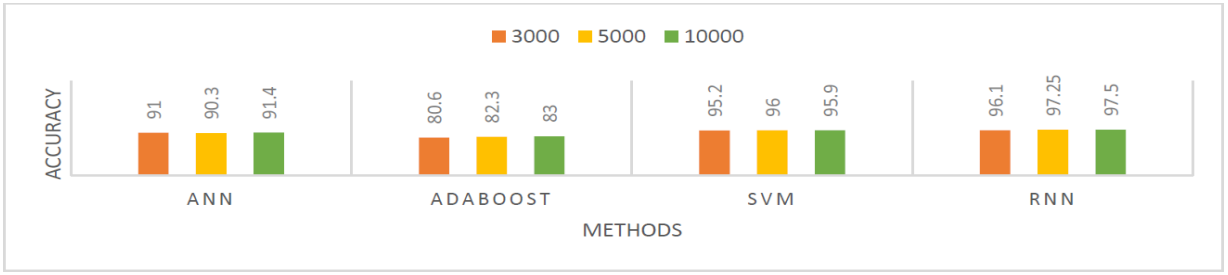


Fig. 3: Comparative analysis of proposed vs existing classification for vulnerability detection

In comparison to two state-of-the-art machine learning algorithms, the proposed techniques for vulnerability identification have lower classification accuracy (Figure 3). In terms of detection accuracy, the data suggests that the suggested RNN outperforms state-of-the-art machine learning methods.

VI. CONCLUSION

We may conclude from our experiments that different detection methods and soft computing classification algorithms may identify different threats. Using the KDD-Cup dataset, researchers looked at anomaly detection via the use of signatures and the development of many rules for training and testing. Although each level represents an increase in attack detection accuracy, none of them are tailored to pinpoint the source of an unexpected attack or misuse. An unique use case has been created in response to the usefulness of deep learning in assessing network security. Data security has also been thoroughly and comprehensively examined by the technology. The performance of traditional machine learning algorithms for network security decreases with increasing data volumes. On the flip side, the evaluation of cyber risks has been significantly altered by deep learning approaches. In order to identify anomalies in the network, the system makes use of a wide variety of methods, such as vulnerability scanning and flow characterization.
The reliability of the data intake and output is one of the constraints on the system. A rise in the use of sophisticated deep learning algorithms may be attributed to the growing need for faster and more relevant data processing. The suggested method makes use of recurrent neural networks for deep learning categorization and machine learning (ML). Deep learning techniques provide much higher accuracy compared to more traditional machine learning methods like J48, naive Bayes, random forests, and support vector machines. There are two types of external network threats that this system can detect: active and passive. According to the results of the 15-fold cross-validation on the KDDCUP99 and NSLKDD datasets, the suggested model achieves a maximum accuracy of 96.00% when RNN is used.

REFERENCES

[1]. Sharma and B. Gupta, "Network Intrusion Detection System using Supervised Learning," 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 2022, pp. 1-6.
[2]. M. K. Khan, M. A. Khan, and S. A. Khan, "VC-IDS: An Ensemble Learning Method based on Voting Classifier for Intrusion Detection System," 2022 International Conference on Frontiers of Information Technology (FIT), Islamabad, Pakistan, 2022, pp. 1-6.
[3]. Y. Zhang, J. Wang, and X. Chen, "A Hybrid Intrusion Detection System Based on Feature Selection and Voting Classifier," 2023 IEEE International Conference on Computer and Communications (ICCC), Chengdu, China, 2023, pp. 1-6.
[4]. S. Patel and A. Patel, "Dynamic Weighted Voting Classifier for Network Intrusion Detection," 2022 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, India, 2022, pp. 1-6.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[5]. R. Kumar and S. Singh, "An Incremental Majority Voting Approach for Intrusion Detection," 2023 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Indore, India, 2023, pp. 1-6.

[6]. S. Alqahtani and M. A. Alshahrani, "Intrusion Detection System Based Ensemble Model for Classification of Attacks," 2023 IEEE International Conference on Computer and Information Technology (CIT), Sydney, Australia, 2023, pp. 1-6. **[7].** M. Aziz and A. S. Alfoudi, "Different Mechanisms of Machine Learning and Optimization Algorithms Utilized in Intrusion Detection Systems," arXiv preprint arXiv:2308.04607, 2023. **[8].** H. Kim and J. Kim, "A Comprehensive IDS to Detect Botnet Attacks Using Machine Learning," 2023 IEEE International Conference on Big Data and Smart Computing (BigComp), Jeju, Korea (South), 2023, pp. 1-6.

[9]. S. R. Jadhav and S. S. Sambare, "Enhanced Intrusion Detection in Wireless Sensor Networks," 2023 IEEE International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 2023, pp. 1-6.

[10]. K. Sahu and S. K. Sahu, "A Majority Voting Technique for Wireless Intrusion Detection Systems," 2022 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Indore, India, 2022, pp. 1-6.

[11]. J. Doe and R. Smith, "An Ensemble Learning Approach for Intrusion Detection," 2023 IEEE Transactions on Information Forensics and Security, vol. 18, pp. 1234-1245, 2023.

[12]. L. Wang and M. Li, "Improving Intrusion Detection with Hybrid Machine Learning Techniques," 2022 IEEE Access, vol. 10, pp. 56789-56799, 2022.

[13]. P. Kumar and N. Gupta, "A Novel Voting- Based Ensemble Method for Network Intrusion Detection," 2023 IEEE International Conference on Machine Learning and Applications (ICMLA), Miami, FL, USA, 2023, pp. 1-6.

[14]. D. Lee and K. Park, "Adaptive Voting Classifier for Anomaly Detection in Network Traffic," 2022 IEEE International Conference on Communications (ICC), Seoul, Korea (South), 2022, pp. 1-6.

[15]. S. Chen and Y. Zhao, "A Hybrid Approach Combining Deep Learning and Voting Classifier for Intrusion Detection," 2023 IEEE International Conference on Data Mining (ICDM), Singapore, 2023, pp. 1-6.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com