INTRUSION DETECTION FRAMEWORK USING EXPLAINABLE MACHINE LEARNING

[1]Chennamsetti Gopi Krishna, [2]Mr. P. Aravind

[1]M.Tech Scholar, Department of Computer Science and Engineering, NRI Institute of Technology, Visadala, Guntur, Andhra Pradesh, India

[2]Assistant Professor, Department of Computer Science and Engineering, NRI Institute of Technology, Visadala, Guntur, Andhra Pradesh, India

ABSTRACT: With the advancements in computer networks and systems, the number of security vulnerabilities and cyber attacks targeting/using these vulnerabilities continues to increase. Consequently, various intrusion detection systems (IDS) have been developed to detect cyber attacks and ensure information security. These models reflect security situations and assist security specialists in identifying the system's vulnerabilities. Network complexity and its many platforms and diverse software products resulted in multiple levels of connectivity, and this complexity of environments offers a severe issue for cybersecurity and overall organizational security. An efficient way to provide computer network security is through intrusion detection systems, which can detect anomalous data in intricate network environments. The structural and dynamic complexity of critical systems cannot be captured by the traditional methods of system vulnerability and risk analysis; cyber-attacks have become more planned and precise and have clear goals targeting weaknesses in systems' security. Therefore, this Intrusion Detection Framework Using Explainable Machine Learning model is trained using certain features, and the learned model is assessed using a testing dataset. The ANN (Artificial Neural Network) algorithm identifies the complex nonlinear relationships between normal and attack patterns. The ANN output is analyzed to detect anomalies in anomaly detector. Therefore, this proposed system detects the attacks accurately.

Keywords: ANN (Artificial Neural Network), Intrusion Detection Systems (IDS), Security, Network Protocols, Cyber Attacks, Cybersecurity

I. INTRODUCTION

Due to a dramatic increase of attacks on machines and network-based services, cyber security has become an essential topic in protecting systems from threats at a local and global scale over the past decades [1]. Although network firewalls and data encryption have already provided basic security for computers and networks, as well as satisfied the requirements of fundamental security, there are still a large number of threats that have gone unnoticed and given rise to detrimental effects on the services as a whole [2]. Intrusions are dangerous threats that require immediate attention. Intruders pose the greatest risk to organizations, particularly to units that require a high level of security such as military bases and airports. Failure to detect intruders inevitably leads to security breaches such as the theft of classified information, gaining unauthorized access, and disguising as an administrator for destructive purposes [3].

According to NSL-KDD [4], there are four major classes of attacks 1) Denial Of Service (DoS) is an attack that floods the target with a massive amount of traffics in order to render the service unavailable abruptly. 2) Probe is an attack that scans and exploits network vulnerabilities in open ports to identify services run by the target. 3) Remote2Local (R2L) is an attack that attempts to exploit the target's vulnerabilities to gain illegal access to local networks. 4) User2Root (U2R) is an attack that attempts to exploit the vulnerabilities of the machine to gain root privileges or take over control of the machines. R2L and U2R attacks are uncommon but pose a more detrimental effect to a system [5].

Thus, advanced techniques for the anomaly-based IDS need to be explored [6]. Even though anomaly-based IDS usually produce high false alarm rates, nowadays it has gained widespread acceptance amongst the IDS research community [7]. One of the best options in the domain is to use a Machine Learning (ML) approach to create an effective model in order to build a pattern recognition of intruders[8].

Attackers may compromise network control mechanisms, leading to malfunctions. The dangerous cyberattacks like Denial of Service (DoS) and Distributed Denial of Service (DDoS) attack the network by attackers. The network resources and channel capacity – reasonable enquiries could be rejected because of excessive use[9]. Computer systems and networks must adopt appropriate security measures to prevent intrusions to eradicate intrusion threats to identify intrusion behaviour. The IDS should extract key elements of computer system, network and compare these elements with normal features. Known intrusion features are determined by intrusion behaviour before it affects the system and network negatively[10].

Thus, the inevitable need of the research community is to focus on developing an efficient Intrusion Detection System (IDS) framework against DDoS attacks with high detection power. The middlebox-based DDoS detection used in conventional systems offers good accuracy, but it causes communication overhead and rigidity[11]. The requirement of customized hardware with software in the middlebox defense technique is incompatible with adaptable network architecture and fails to maintain a global network intelligence [12]. So researchers addressed this issue by a programmable network paradigm called Software Defined Network (SDN) for challenging security threats of DDoS [13] that delivers network intelligence to incorporate the rapid change of network configuration in today's data centers, industry, academic, and IoT era. It helps to provide a holistic, cost-effective, lightweight approach against DDoS attacks without any additional hardware requirements, which is ideal for a modern changing network scenario[14].

II. LITERATURE SURVEY

J. Lee, S. Park, S. Shin, H. Im, J. Lee and S. Lee, et al. [15] develop an intrusion detection system (IDS) that can effectively identify malicious and legitimate CAN messages, as well as an intrusion prevention system (IPS) that can block such malicious messages in real time. In this study, a random-forest-based intrusion detection system (RF-IDS) was proposed and integrated with a CAN controller to design a system that can perform real-time detection and attack blocking. Existing IDS studies aim for high detection performance. This confirmed that the corresponding structure achieved an average detection time of 1.86 μ s and detection accuracy of more than 99%, allowing real-time intrusion blocking. Finally, hardware implementation was achieved by completing the design of the ASIC chip through a multiproject wafer process.

P. Freitas De Araujo-Filho, A. J. Pinheiro, G. Kaddoum, D. R. Campelo and F. L. Soares, et al. [16] propose a novel unsupervised intrusion prevention system (IPS) for automotive CANs that detects and hinders attacks without modifying the architecture of the electronic control units (ECUs) or requiring information that is restricted to car manufacturers. We compare two machine learning algorithms' ability to detect fuzzing and spoofing attacks, and evaluate which of them is most accurate

with the fewest number of data bytes. The fewer data bytes required, the sooner detection can start and the sooner attacking frames can be detected. Experiment results show that our proposed detection mechanism achieves accuracy higher than 99%, F1-scores higher than 97%, and detection times shorter than 80 μs for the types of attacks considered.

I. Aliyu, S. Van Engelenburg, M. B. Mu'Azu, J. Kim and C. G. Lim, et al. [17] investigates the impact of various possible adversarial examples on the BFF (Blockchain-based Federated Forests)-IDS. We also investigated the statistical adversarial detector's effectiveness and resilience in detecting the attacks and subsequent countermeasures by augmenting the model with detected samples. Our investigation results established that BFF-IDS is very vulnerable to adversarial examples attacks. The statistical adversarial detector and the subsequent BFF-IDS augmentation (BFF-IDS(AUG)) provide an effective mechanism against the adversarial examples. Consequently, integrating the statistical adversarial detector and the subsequent BFF-IDS augmentation with the detected adversarial samples provides a sustainable security framework against adversarial examples and other unknown attacks.

S. Racherla, P. Sripathi, N. Faruqui, M. Alamgir Kabir, M. Whaiduzzaman and S. Aziz Shah, et al. [18] introduces Deep-IDS, an innovative and practically deployable Deep Learning (DL)-based IDS. It employs a Long-Short-Term-Memory (LSTM) network comprising 64 LSTM units and is trained on the CIC-IDS2017 dataset. Its streamlined architecture renders Deep-IDS an ideal candidate for edge-server deployment, acting as a guardian between IoT nodes and the Internet against Denial of Service, Distributed Denial of Service, Brute Force, Man-in-the-Middle, and Replay Attacks. A distinctive aspect of this research is the trade-off analysis between the intrusion Detection Rate (DR) and the False Alarm Rate (FAR), facilitating the real-time performance of the Deep-IDS. The system demonstrates an exemplary detection rate of 96.8% at the 70% threshold of DR-FAR trade-off and an overall classification accuracy of 97.67%. Furthermore, Deep-IDS achieves precision, recall, and F1-scores of 97.67%, 98.17%, and 97.91%, respectively.

M. Moukhafi, K. E. Yassini and S. Bri, et al. [19] proposes a novel method of intrusion detection based on pre-processing of training data and a combination PSO (Particle Swarm Optimization) -SMO (Sequential minimal optimization) to develop a model for intrusion detection system. The simulation results show a significant improvement in performances, all tests were realized with the kdd99 data set. compared with other methods based on the same dataset, the proposed model shows high detection performances.

M. H. Bhavsar, Y. B. Bekele, K. Roy, J. C. Kelly and D. Limbrick, et al. [20] proposed FL-IDS model uses embedded devices (such as Raspberry Pi for the client and Jetson Xavier for the server model). The real-time performance of the proposed IDS was evaluated using two different datasets, NSL-KDD and Car-Hacking. We deployed our IDS model on different architectures, testbed 1 (with 2 clients) and testbed 2 (with 4 clients). The model evaluation has been evaluated based on the accuracy, and loss parameters. The results show that the FL-IDS system outperforms traditional centralized learning with machine learning and deep learning approaches regarding accuracy (achieved overall 94% and 99%) and loss (achieved overall 0.28 and 0.009).

These findings contribute to transportation IoT systems security by proposing a robust framework for enhancing the security and privacy of CAVs against cyber threats.

R. Ben Said, Z. Sabir and I. Askerzade et al. [21] created a hybrid Convolutional Neural Network (CNN) and bidirectional long short-term memory (BiLSTM) network to enhance network intrusion detection using binary and multiclass classification. The effectiveness of the proposed model was tested and assessed using the most frequently used datasets (UNSW-NB15 and NSL-KDD). In addition, we used the InSDN dataset, which is specifically dedicated to SDN. The outcomes demonstrate the efficiency of the proposed model in achieving high accuracy and requiring less training time.

A. H. Janabi, T. Kanakis and M. Johnson, et al. [22] presents a new model that offers decentralised processing and exchanges data over an independent channel, in order to solve issues relating to system overload and poor performance. Our model utilises an appropriate feature selection method to reduce the number of extracted features and minimise the data transmitted over the channels. Additionally, the Naive Bayes algorithm has been employed for flow classification purposes, since it is a fast classifier. We successfully implemented our framework, using the Mininet emulator, which provides a suitable networking environment. Evaluations indicate that our proposed system can detect various attacks with an accuracy of 98.46% and nominal decreasing rates of 1.5% in throughput and 0.7% in latency analyses, when the model is implemented in wide range networks.

M. Vishwakarma and N. Kesswani, et al. [23] proposes a stacking ensemble model. The approach integrates a Deep Intrusion Detection System (DIDS) with a Convolutional Neural Network (CNN) and a Long Short-Term Memory (LSTM) model. The Random Forest algorithm is used as a meta-classifier in the stacking process to improve accuracy. The model also addresses the challenge of detecting minority-class attacks in IoT traffic. We evaluate the approach on data derived from the CIC IoT 2022 dataset (pcap files converted to flow records using CICFlowMeter), and demonstrate real-time deployment on a resource-constrained edge device. Furthermore, we incorporate Explainable AI techniques to interpret the model's decisions, thereby improving user trust in the system. Our results show that the proposed model effectively and robustly detects intrusions in IoT environments.

S. Gopikrishnan, P. Jonnalagadda, M. Driss and W. Boulila, et al. [24] presents an Efficient Feature-Selection-based Intrusion Detection System (EFS-IDS) tailored for IoT environments. The framework addresses three significant challenges: feature redundancy, data imbalance, and model generalization through a multistage deep learning pipeline. First, an ensemble feature selection mechanism combines Information Gain, Fast Correlation-Based Filter, and Average Feature Importance to identify a compact yet highly discriminative subset of features. Second, a hybrid balancing strategy integrating SMOTE and Borderline-SMOTE mitigates skewed class distributions, improving recognition of minority attacks. Third, a cost-sensitive CNN–DNN hybrid classifier leverages convolutional layers for localized flow pattern extraction and deep dense layers for global decision modeling, optimized through a weighted cross-entropy loss.

D. Javeed, T. Gao, P. Kumar and A. Jolfaei, et al. [25] proposed IDS is designed by

combining bidirectional long short-term memory networks (BiLSTM), a bidirectional-gated recurrent unit (Bi-GRU), fully connected layers and a softmax classifier to enhance the intrusion detection process in Industry 5.0. We employ the SHapley Additive exPlanations (SHAP) mechanism to interpret and understand the features that contributed the most in the decision of the proposed cyber-resilient IDS. The evaluation of the proposed model using the explainability can ensure that the model is working as expected. The experimental results based on the CICDDoS2019 dataset confirms the superiority of the proposed IDS over some recent approaches.

III. FRAMEWORK OF INTRUSION DETECTION FRAMEWORK USING EXPLAINABLE MACHINE LEARNING

In this section, framework of Intrusion Detection Framework Using Explainable Machine Learning is observed in Figure .1. In this proposed system considers dataset as input that contains normal and attack-related network traffic records. Then missing values, duplicate records, and irrelevant information are removed from the raw data in dataset Pre-processor to convert categorical attributes into numerical form. Data cleaning to removing bad, wrong, or empty network and system log data before security tools analyze it. Standardization in an Intrusion Detection System (IDS) is a data preprocessing step that rescales feature values to have a mean of zero and a standard deviation. Feature selection reduces computing complexity by removing duplicated features and identifying the most pertinent characteristics from retrieved information. The datasplitted into training and testing phases. The model is trained using the chosen features, and the learned model is assessed using the testing dataset. The ANN (Artificial Neural Network) algorithm identifies the complex nonlinear relationships between normal and attack patterns. The ANN output is analyzed to detect anomalies. Final classification is performed by decision for attack detection to determine whether the traffic is Normal or Attack/Intrusion.

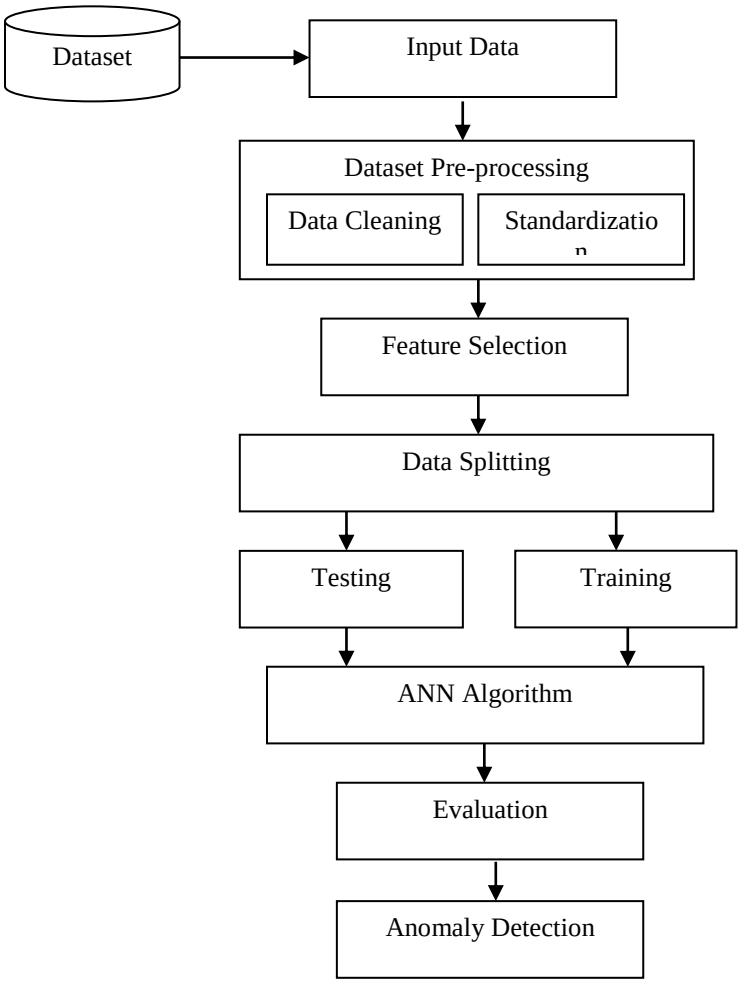

Figure 1. Framework for Intrusion Detection Framework Using Explainable Machine Learning

Data preprocessing is the essential process of cleaning, transforming, and organizing raw data into a structured format so it can be used effectively for data science, machine learning, and analysis. It fixes flaws like missing values, noise, and duplicates. Data Cleaning fixes missing values using

averages or deletion. It removes duplicate rows and fixing types.

In cybersecurity, network datasets (like NSL-KDD or UNSW-NB15) contain features with vastly different scales and units (e.g., packet duration in milliseconds vs. byte counts in the thousands). Our data can be in various formats i.e., numbers (integers) & words (strings), and consider only the numbers in our Dataset. Assume our dataset has random numeric values in the range of 1 to 95,000 (in random order). Just for our understanding consider a small Dataset of barely 10 values with numbers in the given range and randomized order.

Feature selection in a Machine Learning (ML) Intrusion Detection System (IDS) is the process of identifying and keeping only the most relevant network data attributes (like packet size or protocol type), while discarding redundant or noisy data. It is crucial for lowering computational overhead and boosting attack detection accuracy.

The next step is to design several training sets and testing sets with different quality levels for the purpose of validating the effect of data quality on model performance. The quality level of each dataset (training set and testing set) is either clean or unclean. In a clean set of data, we get rid of overlaps and duplicates using our data cleaning method, and in an unclean set of data, we leave the data as is, so there may be duplicates and overlaps. The difference in the data processing procedure for a training set versus a testing set is an extra step of data imbalance handling in the training data. The reason is we do not want data imbalance to affect the model learning capabilities, yet we want a reliable model evaluation in the testing data.

An Artificial Neural Network (ANN) is an algorithmic model inspired by the human brain. It serves as the analytical core that learns non-linear patterns in network traffic to accurately distinguish between safe, legitimate activity and malicious attacks. Traditional, signature-based IDSs struggle because they only recognize previously known threats. ANNs are used in anomaly detection frameworks to drastically improve security.

Intrusion Detection System (IDS) is to identify when a malefactor is attempting to compromise the operation of a system. That is to say, cause the system to operate in a manner which it was not designed to do. This could take the form of a compromise to the confidentiality, availability and integrity of the system and the data stored and controlled by it. Systems could be hosts, servers, Internet of Things (IoT) devices, routers or other intermediary devices. Traditionally, at the highest level, intrusion detection systems fall into one of the following two categories, host based intrusion detection systems (HIDS) and network based intrusion detection systems (NIDS). The former being an individual device detecting a compromise and the latter detecting a compromise in transit over a network. NIDS can be further categorised into anomaly and signature based systems. Signature based systems form the mainstay of commercial network intrusion detection systems with anomaly based still largely a research concept with only a few practical vendor backed examples. Increasingly alerts and other incident information generated via an IDS act as a feed into security information and event management (SIEM) systems, along with other logs and feeds allowing a more complete view of a potential incident to be recorded.

ANNs have been used in a wide variety of classification tasks across many application domains. In contrast to traditional classification methods, such as logistic

regression and discriminant analysis, which require a good understanding of the underlying assumptions of the probability model of the system that produced the data, ANNs are a “black-box” technique capable of adapting to the underlying system model. This makes them particularly useful in fields such as decision support for concealed weapons detection, prediction and classification of Internet traffic, and signature verification where their ability to adapt to the data, especially in high dimensional datasets, overcomes many of the difficulties in model building associated with conventional classification techniques such as decision trees and k-nearest neighbour algorithms.

IV. RESULT ANALYSIS

In this section, result analysis of Intrusion Detection Framework Using Explainable Machine Learning is observed.

The Figure 2, shows home page of Intrusion Detection System for Security Enhancement using machine learning.

Figure 2. Home page

Generating the Model image is shown in Figure 3 for Machine Learning Framework Based Intrusion Detection System for Security Enhancement.

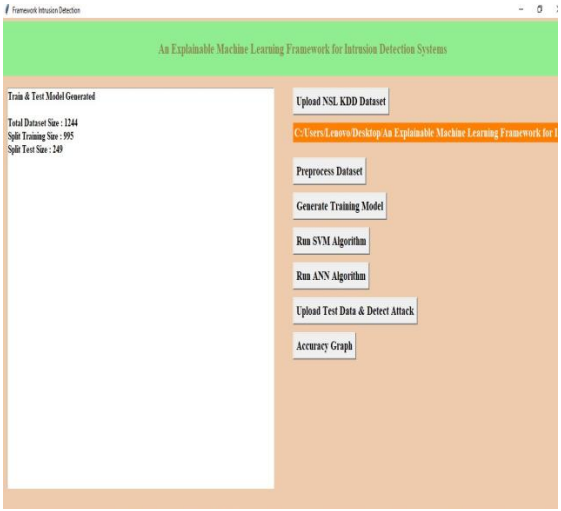

Figure 3. Generating the Model

The Figure 4, shows ANN algorithm applied for Intrusion Detection System for Security Enhancement using machine learning. The ANN output is analyzed to detect anomalies in anomaly detector.

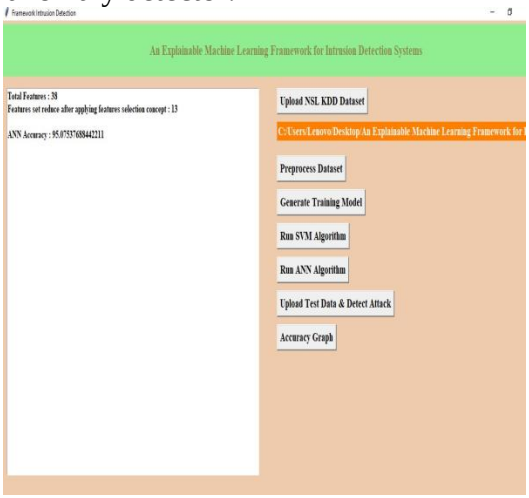

Figure 4. ANN Algorithm Running

V. CONCLUSION

An Intrusion Detection System (IDS) is a software application or device that monitors the system or activities of network for policy violations or malicious activities and generates reports to the management system.

A number of systems may try to prevent an intrusion attempt but this is neither required nor expected of a monitoring system. The main focus of Intrusion detection and prevention systems (IDPS) is to identify the possible incidents, logging information about them and in report attempts. In addition, organizations use IDPS for other purposes, like identifying problems with security policies, deterring individuals and documenting existing threats from infringing security policies. In this Intrusion Detection Framework Using Explainable Machine Learning model, data pre-processing, cleaning, Standardization and selection are integrated along with ANN model. The ANN (Artificial Neural Network) algorithm identifies the complex nonlinear relationships between normal and attack patterns. The ANN output is analyzed and detects anomalies. To determine if the communication is normal or attack/intrusion, the final classification is carried out by the decision for attack detection. By improving threat detection, lowering false positives, and adjusting to changing threats that are dispersed throughout the Internet of Things (IoT), devices, edge nodes, and cloud nodes, this model enhances intrusion detection system (IDS) systems.

VI. REFERENCES

[1] T. Wisanwanichthan and M. Thammawichai, "A Double-Layered Hybrid Approach for Network Intrusion Detection System Using Combined Naive Bayes and SVM," in IEEE Access, vol. 9, pp. 138432-138450, 2021, doi: 10.1109/ACCESS.2021.3118573.

[2] U. S. Musa, M. Chhabra, A. Ali and M. Kaur, "Intrusion Detection System using Machine Learning Techniques: A Review," *2020 International Conference on Smart Electronics and Communication (ICOSEC)*, Trichy, India, 2020, pp. 149-155, doi: 10.1109/ICOSEC49089.2020.9215333.

[3] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, “Intrusion detection system: A comprehensive review,” J. Netw. Comput. Appl., vol. 36, no. 1, pp. 16–24, 2013, doi: 10.1016/j.jnca.2012.09.004.

[4] M. Tavallaee, E. Bagheri, W. Lu and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, Ottawa, ON, Canada, 2009, pp. 1-6, doi: 10.1109/CISDA.2009.5356528.

[5] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha and K. -K. R. Choo, "A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks," in *IEEE Transactions on Emerging Topics in Computing*, vol. 7, no. 2, pp. 314-323, 1 April-June 2019, doi: 10.1109/TETC.2016.2633228.

[6] R. Lippmann, D. Fried, I. Graf, J. Haines, K. Kendall, D. McClung, D. Weber, S. Webster, D. Wyschogrod, R. Cunningham, and M. Zissman, “Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation,” in *Proc. DARPA Inf. Survivability Conf. Expo.*, vol. 2, 2000, pp. 12–26, doi: 10.1109/DISCEX.2000.821506.

[7] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153-1176, Secondquarter 2016, doi: 10.1109/COMST.2015.2494502

[8] F. Salo, M. Injadat, A. B. Nassif, A. Shami and A. Essex, "Data Mining Techniques in Intrusion Detection Systems: A Systematic Literature Review," in *IEEE Access*, vol. 6, pp. 56046-56058, 2018, doi: 10.1109/ACCESS.2018.2872784.

[9] E. -U. -H. Qazi, T. Zia, M. Hamza Faheem, K. Shahzad, M. Imran and Z. Ahmed, "Zero-Touch Network Security

(ZTNS): A Network Intrusion Detection System Based on Deep Learning," in IEEE Access, vol. 12, pp. 141625-141638, 2024, doi: 10.1109/ACCESS.2024.3466470.
[10] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi and R. Ahmad, "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System," in IEEE Access, vol. 10, pp. 99837-99849, 2022, doi: 10.1109/ACCESS.2022.3206425
[11] H. Wang, Q. Jia, D. Fleck, W. Powell, F. Li, and A. Stavrou, "A moving target DDoS defense mechanism," Comput. Commun., vol. 46, pp. 10–21, Jun. 2014, 10.1016/j.comcom.2014.03.009
[12] S. T. Zargar, J. Joshi and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," in *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2046-2069, Fourth Quarter 2013, doi: 10.1109/SURV.2013.031413.00127.
[13] A. Akhunzada, E. Ahmed, A. Gani, M. K. Khan, M. Imran and S. Guizani, "Securing software defined networks: taxonomy, requirements, and open issues," in *IEEE Communications Magazine*, vol. 53, no. 4, pp. 36-44, April 2015, doi: 10.1109/MCOM.2015.7081073.
[14] Z. Shu, J. Wan, D. Li, J. Lin, A. V. Vasilakos, and M. Imran, "Security in software-defined networking: Threats and countermeasures," Mobile Netw. Appl., vol. 21, no. 5, pp. 764–776, Oct. 2016 doi, 10.1007/s11036-016-0676-x.
[15] J. Lee, S. Park, S. Shin, H. Im, J. Lee and S. Lee, "ASIC Design for Real-Time CAN-Bus Intrusion Detection and Prevention System Using Random Forest," in *IEEE Access*, vol. 13, pp. 129856-129869, 2025, doi: 10.1109/ACCESS.2025.3585956.
[16] P. Freitas De Araujo-Filho, A. J. Pinheiro, G. Kaddoum, D. R. Campelo and F. L. Soares, "An Efficient Intrusion Prevention System for CAN: Hindering Cyber-Attacks With a Low-Cost Platform," in *IEEE Access*, vol. 9, pp. 166855-166869, 2021, doi: 10.1109/ACCESS.2021.3136147.
[17] I. Aliyu, S. Van Engelenburg, M. B. Mu'Azu, J. Kim and C. G. Lim, "Statistical Detection of Adversarial Examples in Blockchain-Based Federated Forest In-Vehicle Network Intrusion Detection Systems," in *IEEE Access*, vol. 10, pp. 109366-109384, 2022, doi: 10.1109/ACCESS.2022.3212412.
[18] S. Racherla, P. Sripathi, N. Faruqui, M. Alamgir Kabir, M. Whaiduzzaman and S. Aziz Shah, "Deep-IDS: A Real-Time Intrusion Detector for IoT Nodes Using Deep Learning," in *IEEE Access*, vol. 12, pp. 63584-63597, 2024, doi: 10.1109/ACCESS.2024.3396461.
[19] M. Moukhafi, K. E. Yassini and S. Bri, "A Novel Anomaly Intrusion Detection Based on SMO Optimized by PSO with Pre-Processing of Data Set," in *Journal of Mobile Multimedia*, vol. 13, no. 3-4, pp. 197-209, July 2017, doi: JMM/JMM.2017.11080122.
[20] M. H. Bhavsar, Y. B. Bekele, K. Roy, J. C. Kelly and D. Limbrick, "FL-IDS: Federated Learning-Based Intrusion Detection System Using Edge Devices for Transportation IoT," in *IEEE Access*, vol. 12, pp. 52215-52226, 2024, doi: 10.1109/ACCESS.2024.3386631.
[21] R. Ben Said, Z. Sabir and I. Askerzade, "CNN-BiLSTM: A Hybrid Deep Learning Approach for Network Intrusion Detection System in Software-Defined Networking With Hybrid Feature Selection," in *IEEE Access*, vol. 11, pp. 138732-138747, 2023, doi: 10.1109/ACCESS.2023.3340142
[22] A. H. Janabi, T. Kanakis and M. Johnson, "Overhead Reduction Technique for Software-Defined Network Based Intrusion Detection Systems," in *IEEE Access*, vol. 10, pp. 66481-66491, 2022, doi: 10.1109/ACCESS.2022.3184722.

[23] M. Vishwakarma and N. Kesswani, "StaEn-IDS: An Explainable Stacking Ensemble Deep Neural Network-Based Intrusion Detection System for IoT," in *IEEE Access*, vol. 13, pp. 109713-109728, 2025, doi: 10.1109/ACCESS.2025.3582391.

[24] S. Gopikrishnan, P. Jonnalagadda, M. Driss and W. Boulila, "EFS-IDS: An Enhanced Feature-Selective Intrusion Detection System for Imbalanced IoT Traffic Data," in *IEEE Open Journal of the Communications Society*, vol. 6, pp. 9673-9695, 2025, doi: 10.1109/OJCOMS.2025.3630471.

[25] D. Javeed, T. Gao, P. Kumar and A. Jolfaei, "An Explainable and Resilient Intrusion Detection System for Industry 5.0," in *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1342-1350, Feb. 2024, doi: 10.1109/TCE.2023.3283704.