International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

A Study on Network Intrusion Detection System

Mohammed Kaif[1], Prajwal P[2], Laxmi V[3]

[1,2]Student, Information Science and Engineering, BNM Institute of Technology/VTU Karnataka, India
[3]Associate Professor, Information Science and Engineering, BNM Institute of Technology/VTU Karnataka, India

1. ABSTRACT

An extensive overview of network intrusion detection systems (NIDS) is provided in the abstract, emphasizing the importance of these systems for protecting information and communication technology (ICT) networks.

It summarizes the research in three primary areas: attack kinds, technologies, and datasets. NIDS models have been trained and tested on a variety of datasets, including the KDD dataset, with the goal of improving classification rates and computational effectiveness. The survey describes the various capabilities and uses of a variety of NIDS technologies, such as ABTrap, RNN, CNN, Naive Bayes, Random Forest, and Decision Trees.

Furthermore, the abstract discusses the frequency of Denial of Service (DoS) and Distributed Denial of Service (DDoS) assaults, emphasizing the necessity of strong defence mechanisms in Network Intrusion Detection Systems (NIDS) to guarantee network availability and security against constantly changing cyberthreats.

2. INTRODUCTION

Network intrusion detection systems, or NIDS, are essential parts of cybersecurity architecture that guard against hostile activity on information and communication technology (ICT) networks. In order to protect the availability and integrity of network resources, network intrusion detection systems (NIDS) continuously monitor network traffic. They do this by using advanced algorithms to identify and react to suspicious activity. The creation of efficient NIDS is becoming more and more essential to preserving the security posture of networks and enterprises as cyber attacks grow in sophistication and intricacy. There are two main approaches to Network Intrusion Detection Systems (NIDS): anomaly-based and misuse-based. Whereas misuse-based systems rely on predetermined signatures to identify known attacks, anomaly-based systems examine network traffic patterns to find departures from typical activity. The anomaly-based detection system offers versatility in identifying unknown threats, while the misuse-based detection system is effective in recognizing established attack patterns. These two systems work well together. Through creative approaches and procedures, NIDS technologies are always evolving to improve detection capabilities and resilience to new threats.

Datasets:

The review of the literature highlights the increasing importance of anomaly detection in cybersecurity research, especially in light of the shortcomings of signature-based intrusion detection systems (IDSs) in terms of spotting new types of assaults. The extensively used KDD Cup '99 dataset has been examined through in-depth statistical analysis, exposing two crucial problems influencing the assessment of anomaly

detection techniques. The abundance of duplicate records and the simplicity of categorizing entries are two of these problems, which skew learning algorithms and make evaluation procedures more difficult.

In order to rectify these deficiencies, a subset of the original KDD dataset—the NSL-KDD dataset—was created. Redundancies are removed from this dataset, giving evaluation-ready data that is cleaner.Furthermore, KDD Cup '99, NSL-KDD, and Kyoto 2006+ are three well-known datasets in intrusion detection research that are covered in the paper. Although KDD Cup '99 is still a popular benchmark, NSL-KDD and Kyoto 2006+ improve the representativeness of intrusion detection models by offering cleaner data and actual network traffic statistics, which addresses the shortcomings of KDD Cup '99.

The survey emphasizes how important intrusion detection systems (IDSs) are for protecting computer networks from malicious activity. Both host-based and network-based IDSs are essential. These datasets are used by researchers to create efficient intrusion detection systems (IDSs) that can handle changing cyberthreats in contemporary networked environments. As a result, the availability of datasets like Kyoto 2006+, NSL-KDD, and KDD Cup '99 makes it easier to create and assess reliable intrusion detection techniques, which makes a substantial contribution to cybersecurity research and defensive mechanisms.

Technologies:

Utilizing a variety of technologies to improve detection efficiency and accuracy is a key component of NIDS implementation. Promising approaches in NIDS development include advanced techniques like Random Forest, Decision Trees, Recurrent Neural Networks (RNNs), Convolutional Neural Networks (CNNs), Feature reduction using Recurrent Neural Networks (RNNs), and feature reduction using Naive Bayes. While feature reduction techniques using Naive Bayes, RNNs, CNNs, Random Forest, and Decision Trees optimize the classification process by selecting the most relevant features, thereby improving detection accuracy and reducing computational complexity, ABTrap provides real-time anomaly detection by effectively analysing network traffic patterns. These technologies support the continuous development of NIDS capabilities, as do more established techniques like rule-based systems and signature-based detection algorithms.

Methodologies:

In this overview of the literature, numerous studies on network intrusion detection systems (NIDSs) and the effectiveness of ML and DL algorithms in identifying cyberattacks are thoroughly examined.

The efficiency and performance of ML-based NIDSs are examined in the first study in relation to traffic sampling. This illustrates that even at modest sampling rates, harmful flows of shorter sizes have a higher probability of being undiscovered. The combination of the random forest classifier and the systematic linear sampler, SketFlow, shows better detection rates and lower false alarm rates. It also investigates various sampling strategies and classifiers.

A novel two-stage deep learning model for network intrusion detection called LSTM-AE is proposed in the second study. By using the CICIDS2017 and CSE-CICDIS2018 datasets to identify the ideal network parameters, it solves the need for updated datasets. According to experimental findings, attacks in contemporary circumstances can be detected by the hybrid LSTM-AE model with good accuracy.

In order to address the issue of out-of-date datasets in NIDSs, the third study presents the AB-TRAP framework, which creates updated attack and legitimate datasets. Case studies show excellent performance with low CPU and RAM use, guaranteeing reproducibility and resolving issues with model realization and deployment.

In order to improve network security, effective intrusion detection is essential, as demonstrated by the fourth study's comparative comparison of machine learning-based models and intrusion detection systems. It proposes a decision tree-based detection framework, leveraging findings from a comparative survey to build an effective model.

In the fifth study, the CIPMAIDS2023-1 dataset is introduced and the growing demand for trustworthy NIDSs is discussed. With a weighted F1-score of 98.24%, it shows potential for improving NIDS performance and suggests an ensemble strategy based on stacking.

The aforementioned works emphasize the significance of machine learning and deep learning techniques in network intrusion detection systems (NIDSs) and showcase developments in intrusion detection approaches, dataset application, and model performance assessment.

Types of attacks

The review of the literature provides information on Distributed Denial of Service (DDoS) and Denial of Service (DoS) attacks, their effects, analysis, and defenses in IPv4 and IPv6 networks. Using Software Defined Networking (SDN) technology, the work presents a unique Source-based DDoS defense mechanism designed for fog and cloud computing environments. The technique enhances network resilience against DDoS threats by efficiently identifying and blocking malicious packets through the use of deep learning (DL) based detection. In fog and cloud computing settings, this method guarantees continuous service delivery while resolving important security issues with availability.

Different DoS and DDoS attack types are categorized according to their impact, analysis, and countermeasures in a different study. These attacks, which include TCP Syn Flood, UDP Flood, ICMP Flood, Smurf, and Incomplete HTTP Requests, take advantage of flaws in TCP/IP protocols. The spread nature of DDoS attacks, which are coordinated by numerous compromised machines, presents additional difficulties. The research offers important insights into the nature of these dangers by classifying attacks according to network protocols and layers.

The work highlights how disruptive DoS assaults are and how they target the availability of system and network resources. assaults are further divided into IPv4 and IPv6-based categories, with subcategories for Layer-4 and Layer-7 assaults. IPv6 Neighbor Discovery Protocol-based attacks are given special attention.By discussing attacker methods and vulnerabilities exploited, the paper sets the stage for subsequent sections, focusing on attack types and countermeasures to bolster cybersecurity.

When taken as a whole, these studies provide a thorough understanding of the dynamic environment surrounding DoS and DDoS attacks. They also emphasize the significance of efficient mitigation techniques, especially in fog and cloud computing environments, to guarantee continuous service delivery and uphold network security.

3. RELATED WORKS

[1] The study offers a perceptive examination of the development and history of intrusion detection systems (IDS), charting the technology's beginnings in the 1970s and examining present and emerging trends. With discussions on various methods and instruments used in network defence, including Defence-in-Depth and Intrusion Detection Systems (IDS), it emphasizes the growing significance of network security. The study explores the evolution of IDS, encompassing the foundational publications of James P. Anderson and the innovative endeavours of Dorothy Denning and Peter Neumann in establishing the initial real-time IDS prototype, IDES.

The field of intrusion detection has grown significantly in the last few years, and a wide range of IDS have been created to address changing security requirements. In the middle of the 1990s, commercial systems like Netranger and RealSecure were a major factor in the rise in popularity of network-based IDS. The advent of behaviour-based IDS in response to novel and sophisticated assaults, as well as the shortcomings of knowledge-based IDS, are also discussed in the study. It talks about the research community's continuous efforts to solve problems with high-speed networks and the move toward host-based intrusion detection systems to keep up with network growth and speed.

[2] The identification of novel threats by signature-based intrusion detection systems (IDSs) has been hindered. Consequently, anomaly detection has gained considerable attention in cybersecurity research. Two crucial problems impacting the assessment of anomaly detection techniques have been identified through statistical analysis of the extensively utilized KDDCUP'99 dataset. An NSL-KDD dataset, which consists of certain records from the entire KDD dataset, has been offered as a solution to the problems.

The usage of computer networks and applications has increased, and with it has grown the significance of network security. Intruder detection systems (IDSs) are essential for spotting irregularities and attacks even if security flaws are present in most computer systems. Because anomaly detection can handle new threats, academic research frequently favors it over misuse-based detection, which is the preference of commercial products.

Modern IDS systems and commercial products have not embraced anomaly detection techniques, despite research publications reporting high detection rates. This disparity spurred scientists to investigate anomaly detection in greater detail, which exposed flaws in the widely used KDDCUP'99 dataset for assessment.

The KDD dataset's main problems are that it has a lot of redundant records and that classifying its records is simple. This redundancy makes it difficult to evaluate various intrusion detection techniques since it biases learning algorithms and complicates evaluation. New train and test sets free from these flaws have been produced as a result of solutions to these problems being put forth. The NSL-KDD dataset is accessible to the general public and is used as a standard for assessing intrusion detection techniques.

[3] An overview of three datasets—KDD Cup '99, NSL-KDD, and Kyoto 2006+—that are often utilized in intrusion detection research is given in this study. KDD Cup '99 has five million recordings with 41 features apiece, classifying attacks into four groups. However, it is limited by redundant records and simulation-based record production. Kyoto 2006+ provides real network traffic data collected over three years, improving its representativeness, whereas NSL-KDD tackles these problems by eliminating duplicates.

Computer networks need to be kept safe from unwanted activity, and intrusion detection systems (IDSs) are essential for this. Whereas network-based IDSs examine packet content for anomalous activity, host-based IDSs keep an eye on system changes. Effective IDSs are developed by researchers using datasets such as Kyoto 2006+, NSL-KDD, and KDD Cup '99. While KDD Cup ‘99 serves as a benchmark, NSL-KDD and Kyoto 2006+ offer solutions to its limitations by providing cleaner data and real network traffic information. These datasets are essential for addressing evolving cyber threats in modern networked environments.

[4] The study looks into how machine learning (ML)-based network intrusion detection systems (NIDSs) perform and operate in relation to packet sampling. The suggested evaluation approach, in contrast to earlier studies, is made to be resilient in a variety of flow export stage conditions, offering a thorough evaluation of NIDS performance even when sampling is present. Malicious flows with smaller sizes are

shown to have a higher chance of being undiscovered during sampling trials, even at low sample rates as 1/10 and 1/100.

The impact of different sampling strategies on the false alarm and NIDS detection rates is further investigated in this study. Three sample rates (1/10, 1/100, and 1/1000), four distinct sampling techniques, and three classifiers (two tree-based and one deep learning based) are taken into consideration. The results show that non-linear samplers like Sketch Guided and Fast Filtered sampling are not as effective as the systematic linear sampler SketFlow. Furthermore, when paired with SketchFlow sampling, the random forest classifier exhibits better detection rates and reduced false alarm rates at various sampling rates when compared to alternative sampler-classifier combinations. Regarding the impact of packet sampling on the performance of ML-based NIDS, the findings provide insightful information to researchers and network practitioners.

[5] Assessing intrusion detection systems (IDS) has become a common use of machine learning and deep learning techniques with the goal of quickly and automatically identifying and categorizing cyberattacks on hosts and networks. The cybersecurity sector faces more and more obstacles as cyberattacks become more sophisticated and varied, which calls for an all-encompassing intervention. Numerous publicly available intrusion detection datasets are available, however no previous study has looked closely at how suggested models perform on these datasets. It is crucial to routinely update and benchmark these datasets since assaults are dynamic and their methods are always changing.

In order to create a versatile and efficient IDS, deep neural network (DNN) and convolutional neural network (CNN) models are examined in this article as forms of deep learning models. These models are put up against a suggested model that can identify cyberattacks. The development of intrusion detection systems (IDSs) and the assessment of the many datasets generated over time are essential due to the ever-changing nature of network behavior and the explosive increase of attacks. In order to detect attacks, the research suggests a novel two-stage deep learning technique that combines auto-encoders (AE) with long-short-term memory (LSTM). The CICIDS2017 and CSE-CICDIS2018 datasets are used to estimate the ideal network parameters for the suggested LSTM-AE model. The outcomes of the experiments show that the hybrid model works effectively and may be used to identify attacks in contemporary situations.

[6] The AB-TRAP framework resolves operational issues for full implementation and allows the use of updated network traffic, hence resolving the issue of obsolete datasets in network intrusion detection systems (NIDSs). Creating attack and legitimate datasets, developing machine learning models, putting the models into practice, and assessing post-deployment performance are the five processes involved.

According to case studies, the internet case used eight machine learning algorithms and, with an average overhead of 1.4% CPU and 3.6% RAM on user-space in a single-board computer, achieved an average f1-score of 0.95 and an average area under the ROC curve of 0.98. The LAN case used a decision tree [7] model and achieved these results with minimal CPU and RAM usage. The framework uses the most recent network traffic and attacks, guarantees reproducibility, and fully handles model realization and deployment issues.

[8] The review study emphasizes how difficult it is becoming to reliably detect intrusions due to cyber-attacks, endangering the confidentiality, integrity, and availability of data. It covers the most recent IDS taxonomy, intrusion detection methods, and widely used assessment datasets in addition to the evasion strategies utilized by adversaries. By making improvements to IDSs, researchers want to improve network security by reducing false positives, properly detecting attackers, and identifying new threats. Techniques

for deep learning (DL)[9] and machine learning (ML) have demonstrated promise in effectively identifying network intrusions.

The study examines the most recent developments and trends in machine learning (ML) and deep learning (DL)-based network intrusion detection systems (NIDSs), with an emphasis on methodology, assessment metrics, and dataset selection. It identifies research roadblocks and suggests a paradigm for future study to overcome methodological flaws. Combining results from a comparison survey, the decision tree—which is renowned for its speed and ease of use—is proposed as a model for identifying result abnormalities. The purpose of the study is to provide light on how to create a detection framework based on decision trees that works well.

[10] The study tackles the growing demand for precise and dependable network defence mechanisms, especially given the rise in interconnected device communication. When it comes to identifying suspicious or malicious network activity, network intrusion detection systems, or NDISs, are essential. By creating a fresh dataset, CIPMAIDS2023-1, which solves shortcomings in historical NIDS datasets like CICIDS2017[11], the study seeks to overcome some of the difficulties faced by anomaly-based NIDSs.

The study presents an ensemble strategy based on stacking that is intended to surpass the state-of-the-art NIDS techniques as of right now. A network architecture built with graphical network simulator-3 (GNS-3) was subjected to a variety of attack scenarios and benign user traffic. Using cicflowmeter, key flow features were identified, and the traffic data was subjected to a number of machine learning techniques. Based on the results, the most promising way for improving NIDS performance is the stacking-based ensemble approach, which yields the greatest weighted F1-score of 98.24%.

[12] The study presents a unique Source-based DDoS prevention mechanism that makes use of Software Defined Networking (SDN) technology and is intended for fog and cloud computing environments. By preventing DDoS assaults, which have the potential to disrupt services, it tackles the crucial security issue of guaranteeing availability in fog computing. To improve network resilience against DDoS attacks, the suggested approach uses deep learning (DL) based detection to recognize and stop harmful packets. In order to effectively detect and mitigate aberrant network traffic at the Network/Transport level, the SDN controller is crucial to the DDoS defender module's deployment.

Security and availability are crucial in cloud and fog computing, but DDoS attacks present serious difficulties. In order to identify and counteract such attacks, the article suggests a source-based DDoS defensive mechanism that makes use of SDN technologies. The method effectively filters out harmful traffic, preventing it from reaching cloud resources, by utilizing deep learning for packet inspection. In order to prove the effectiveness of the suggested strategy in thwarting DDoS attacks and guaranteeing continuous service delivery in fog and cloud computing environments, the paper describes the system model and experimental setup.

[13] This paper describes how Denial of Service (DoS) and Distributed Denial of Service (DDoS) assaults are classified, with an emphasis on the analysis, impact, and countermeasures of these attacks on IPv4 and IPv6 networks. DoS attacks come in many forms and take advantage of flaws in TCP/IP protocols. These flaws include TCP Syn Flood, UDP Flood, ICMP Flood, Smurf, and Incomplete HTTP Requests. Because DDoS attacks are dispersed, they present additional obstacles. These attacks use several compromised machines operating as zombies under a master controller. In order to shed light on the characteristics of these risks, the article classifies attacks according to network protocols and layers.

The paper's introduction gives basic information on denial-of-service (DoS) attacks, highlighting their goal of interfering with network and system resources. Since availability requires less complex access,

attackers target it. The study divides attacks into two categories: IPv4 and IPv6-based, and then further breaks them down into Layer-4 and Layer-7 assaults. It pays particular attention to attacks that are based on the IPv6 Neighbour Discovery Protocol. The paper lays the groundwork for later sections that explore attack types and countermeasures with the goal of improving cybersecurity by talking about the techniques employed by attackers and the vulnerabilities they exploit.

[14] In order to improve intrusion detection systems' (IDS) effectiveness, the research focuses on feature selection, which helps to address the problem of effective intrusion detection. The growing global population of Internet users and network-based apps makes unwanted activity a serious danger. The Feature Vitality Based Reduction Method (FVBRM), a novel strategy to find critical features for efficient network intrusion detection, is proposed in this article along with an evaluation of mainstream feature selection techniques. The study intends to improve network security against diverse threats and expedite intrusion detection procedures by using these techniques and employing the naive Bayes classifier on smaller datasets.

The paper explores aspects impacting the performance of the naive Bayes[15] model and emphasizes the significance of feature selection in preserving resource integrity, secrecy, and availability in networked contexts. IDS performance is much improved by the decreased attributes that were chosen, according to the evaluation conducted on the NSL KDD dataset, for all attack types. These results open the door for stronger security measures in networked systems and further our understanding of intrusion detection strategies.

[16] The study presents a three-layer Recurrent Neural Network (RNN) architecture designed to increase classification rates, especially in R2L attacks, for misuse-based Intrusion Detection Systems (IDS) by classifying input attributes and attack types. The suggested model uses the KDD dataset to show better Detection Rate (DR) and Cost Per Example (CPE) than previous efforts, using partial connections in the RNN layers resulting in less computational complexity and faster training.

The paper emphasizes the significance of soft computing techniques like Artificial Neural Networks (ANNs) and fuzzy logic by classifying intrusion detection strategies into statistical-based, knowledge-based, and machine learning approaches. In comparison to comparable techniques, the suggested reduced-size RNN model performs better and achieves higher FAR metrics while retaining a high level of classification accuracy, especially in detecting R2L attacks. The study offers a thorough analysis of the architecture, experimental design, and outcomes of the suggested model, demonstrating its efficacy in enhancing intrusion detection performance.

4. CONCLUSION

The literature review includes a number of important findings about network intrusion detection systems (NIDS) and the datasets that were utilized in the analysis. Initially, the extensively utilized KDD Cup '99 dataset displays deficiencies such intricacy, redundant entries, and an uneven dispersion of attacks. The NSL-KDD dataset was developed in response to these problems, offering an improved level of balance and dependability in the dataset used to assess IDSs. NSL-KDD is a useful benchmark for comparing intrusion detection techniques, even if both datasets are simulations and might not accurately depict actual networks.

To address data imbalance and the effect of sampling on performance, a unique assessment framework for Machine Learning-based NIDS was also presented. Even when sampling is present, the methodology enables a thorough evaluation of NIDS performance. Additionally, the two-stage deep learning method

known as the LSTM-AE model showed enhanced performance in identifying assaults, especially when it was trained and evaluated using datasets such as CICIDS2017 and CSE-CICIDS2018.

Additionally, the AB-TRAP framework addresses the difficulty of adjusting to novel threats and changing network traffic by providing a methodical way to developing and deploying NIDS. AB-TRAP makes it easier to create reliable NIDS systems by offering a pipeline for developing, instructing, deploying, and assessing protection modules.

The survey offers a thorough rundown of AI-based NIDS, emphasizing how DL-based techniques might enhance detection accuracy. It highlights these techniques' potential to improve network security while discussing the challenges of applying them in real-time network intrusion detection systems (NIDS) due to computing needs.

Moreover, an RNN model with partial connectivity was suggested for IDS based on abuse, demonstrating enhanced classification performance, particularly in relation to R2L assaults. In addition, the study provides experimental results, countermeasures, and a thorough classification and analysis of DoS and DDoS assaults under IPv4 and IPv6.

Ultimately, these results offer insightful information on the difficulties and developments in network intrusion detection, giving researchers a path forward for future study aimed at improving the performance of NIDS and dataset evaluation techniques.

5. REFERENCES

1. G. Bruneau, "The History and Evolution of Intrusion Detection," GSEC Version 1.2f, 2021, SANS Institute.
2. D. D. Protić, "Review of KDD Cup '99, NSL-KDD and Kyoto 2006+ Datasets," Serbian Armed Forces, General Staff, Department for Telecommunication and Informatics (J-6), Center for Applied Mathematics and Electronics, Belgrade, Republic of Serbia.
3. M. Tavallaee, E. Bagheri, W. Lu, and A.-A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set."
4. J. Alikhanov, M. Abuhamad, R. Jang, D. Mohaisen, D. Nyang, Y. Noh, "Investigating the Effect of Traffic Sampling on Machine Learning-Based Network Intrusion Detection Approaches," Department of Computer Science, Wayne State University, Detroit, MI, USA, Department of Computer Science, Loyola University Chicago, Chicago, IL, USA, 2023.
5. H. Vanlalruata, H. Nhung-Nguyen, J. Hussain, and A. Yonghwa-Kim, "A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE," Department of Mathematics and Computer Science, Mizoram University, Aizawl, India, Department of Information Technology, Viet Tri University of Industry, Viet Tri, Vietnam, 2023.
6. G. D. C. Bertoli, A. L. D. Santos, F. A. N. Verri, L. A. Pereira Júnior, and O. Saotome, "An End-to-End Framework for Machine Learning-Based Network Intrusion Detection System," Computer Science Division, Aeronautics Institute of Technology (ITA), São José dos Campos, Brazil, Electronics Engineering Division, Aeronautics Institute of Technology (ITA), São José dos Campos, Brazil, 2021.
7. Harsh H. Patel, Purvi Prajapati, Study and Analysis of Decision Tree Based Classification Algorithms, International Journal of Computer Sciences and Engineering October 2018
8. A. Zahedi, M. M. Islam, and M. N. Huda, "Comparative Analysis of Intrusion Detection Systems and Machine Learning-Based Model Analysis Through Decision Tree," Department of Computer Science

and Engineering, United International University, Dhaka, Bangladesh, 2023.
9. Aslam, S., Herodotou, H., Mohsin, S.M., Javaid, N., Ashraf, N.,Aslam, S.: A survey on deep learning methods for power load and renewable energy forecasting in smart microgrids. Renew. Sustain. Energy Rev. 144, 110992 (2021)
10. M. Ali et al., "Effective Network Intrusion Detection using Stacking-Based Ensemble Approach," *International Journal of Information Security*, 2023.
11. Sharafaldin,I.,Lashkari,A.H.,Ghorbani,A.A.:A detailed analysis of the cicids2017 data set. Commun. Comput. Inf. Sci. 977, 172 188 (2019)
12. R. Priyadarshini and R. K. Barik, "A Deep Learning Based Intelligent Framework to Mitigate DDoS Attack in Fog Environment," KIIT University, Bhubaneswar, India.
13. N. Tripathi and B. Mehtre, "DoS and DDoS Attacks: Impact, Analysis and Countermeasures," December 2013.
14. S. Mukherjee and N. Sharma, "C3IT-2012 Intrusion Detection using Naive Bayes Classifier with Feature Reduction."
15. Wafa' S.Al-Sharafat, and Reyadh Naoum "Development of Genetic-based Machine Learning for Network Intrusion Detection" World Academy of Science, Engineering and Technology 55, 2009
16. "Intrusion Detection using Reduced-Size RNN based on Feature Grouping," *Neural Computing and Applications*, vol. 21, no. 6, pp. 1-6, Sep. 2012, doi:10.1007/s00521-010-0487-