Security Framework for Detection of Denial of Service (DoS) Attack on Virtual Private Networks for Efficient Data Transmission

Anthony Edet*[1], Uduakobong Udonna[2], Immaculata Attih[1], and Anietie Uwah[3]
[1]Akwa Ibom State University, Mkpat Enin, Nigeria.
[2]Akwa Ibom State Polytechnic, Ikot Ekpene, Nigeria
[3]National Open University of Nigeria, Nigeria
[1]anthonyedet73@gmail.com, [1]immaculataattih@aksu.edu.ng [3]uwahanietie@gmail.com

DOI: 10.56201/rjpst.v7.no1.2024.pg71.81

Abstract
This study delves into the problem of detecting Denial-of-Service (DoS) attacks on Virtual Private Network (VPN) servers and the detrimental impact of such attacks on network functionality. A DoS attack aims to overwhelm a server, rendering it incapable of providing services to legitimate users. A VPN, on the other hand, serves as a secure conduit for data transmission over the internet. DoS attacks on VPN servers disrupt the seamless flow of communication, causing potential data breaches and compromising the confidentiality, integrity, and availability of network resources. The adverse effects of DoS attacks on VPN servers are profound, ranging from service degradation to complete unavailability. Such disruptions can lead to a breakdown in communication channels, hindering user access to critical resources. Our approach to tackling this challenge involves a meticulous examination of key data features, including Traffic-Volume, Packet-Rate, Traffic-Diversity, Connection-Attempts, Connection-Duration, Protocol-Analysis, and Packet-Size-Distribution. Our dataset is sourced directly from a live server, our study employs the K-Nearest Neighbors (KNN) classification algorithm, to model and identify patterns associated with DoS attacks. Our findings reveal a high accuracy of 94% in detecting DoS attacks using the KNN model, showcasing the efficacy of our approach. The utilization of real-world data enhances the relevance and applicability of our research in practical cybersecurity scenarios.

Keywords: *DoS, VPN, Cybersecurity, KNN*

1.0 Introduction

The increasing reliance on virtual private networks (VPNs) for secure data transmission has been paralleled by a rising cyber threat (Maonan, 2021), particularly in the form of Denial of Service (DoS) attacks (Ramos et al., 2022). VPNs are crucial for protecting sensitive data during transmission (Abugabah, et al., 2020), and their adoption has soared due to the growing need for secure remote work(Sajogo et al, 2023), (Ali et al, 2021), data access(Alliche et al., 2023), and communication(Elluri et al., 2023). However, the vulnerability of VPNs to DoS attacks poses a significant challenge to data security and uninterrupted services(Islam et al., 2023). Denial of Service attacks, which encompass Distributed Denial of Service (DDoS) attacks as a more potent variant, have emerged as persistent threats in the cybersecurity

space(Maghsoudlou et al., 2023), (Naas et al., 2023). These attacks overload the target network or system with an excessive volume of requests, rendering it unresponsive or unavailable to legitimate users (Raza et al., 2022), (Roh et al., 2021). In the context of VPNs, DoS attacks can disrupt secure data transmission, leading to data breaches (Inyang & Umoren, 2023), financial losses, and damage to an organization's reputation(Schumann et al., 2022). Traditional security measures such as firewalls and intrusion detection systems (IDS) are often insufficient to thwart DoS attacks, which are becoming increasingly sophisticated and diverse(Balasubramanian et al., 2022). The need for a proactive and adaptive approach to detect and mitigate DoS attacks in VPNs has given rise to the integration of machine learning techniques into VPN security solutions. Machine learning has demonstrated its efficacy in various cybersecurity domains(Diwen et al., 2022), including anomaly detection(Sriboonruang et al., 2022), pattern recognition(Villegas-Ch et al., 2022), and behavioral analysis. By using machine learning algorithms, it becomes possible to establish a dynamic and intelligent DoS attacker detection system tailored to VPN environments. Such a system can learn from historical attack data, adapt to emerging attack patterns(Abugabah et al., 2020), and ensure uninterrupted and secure data transmission(Vagaš et al., 2019). The central premise of a DoS attacker detection system based on machine learning as proposed in this research is to differentiate between legitimate network traffic and malicious attack traffic on VPN network (Umoren & Inyang, 2021). This is achieved by training machine learning models on labeled datasets (Inyang & Umoren, 2023), where historical network traffic data is categorized as normal or attack traffic. Once trained, these models can classify incoming traffic (Uwah & Edet, 2024), identifying and mitigating DoS attacks as they occur. The significance of this research lies in its potential to bolster VPN security and protect sensitive data in an era when remote work and online communication have become ubiquitous. A robust DoS attacker detection system not only safeguards the integrity of VPNs but also ensures that organizations can maintain the confidentiality and availability of their data (Edet et al., 2024), even in the face of evolving cyber threats. This research endeavor aims to move into developing a DoS attacker detection system for VPN security using machine learning. The intersection of VPN security and machine learning offers a promising avenue to address the persistent challenge of DoS attacks. By developing a DoS attacker detection system tailored to VPN environments, organizations can enhance their data transmission security (Edet & Ansa, 2023), (Ekong et al., 2023) protect against disruptive attacks, and ensure the seamless operation of their critical communication channels. This research endeavors to contribute valuable insights and solutions to strengthen the defense against DoS threats in the VPN space.

2.0 Related Work

Previous research on VPN user detection in a network has been driven by the need to address the security, privacy, and network management challenges posed by VPN usage. These studies have explored various techniques and strategies to distinguish VPN users from regular network users and to develop effective means of identifying and managing VPN connections. Behavioral analysis has been a prominent focus in previous research. By studying the behavior of network users, researchers have aimed to identify patterns associated with VPN usage(Raza *et al.* , 2022). This includes analyzing factors such as session durations, the volume and frequency of data transfers, and communication patterns. These behavioral models can help in detecting anomalies that may signify the use of a VPN, which can be crucial for identifying potential security threats. Traffic analysis is another area of research where efforts have been

made to distinguish VPN traffic from regular network traffic. VPNs often utilize specific ports and protocols, leaving distinct traces in network traffic (Aniss *et al.* , 2023). Researchers have developed methods to analyze these traffic patterns and use them as indicators for detecting VPN connections. By examining the unique characteristics of VPN traffic, network administrators can gain insights into who is using VPNs within their network. Machine learning and artificial intelligence (AI) have played a pivotal role in advancing VPN user detection techniques. These technologies can process and analyze vast amounts of data to identify hidden patterns and trends associated with VPN usage. Machine learning models, such as decision trees, support vector machines (SVM), and neural networks, have been employed to develop predictive models for VPN detection. These models can adapt and learn from new data, enhancing their accuracy in identifying VPN users (Lavanya *et al.* , 2023). DNS (Domain Name System) analysis is another avenue of research. DNS queries made by users can provide valuable insights into their network activities. Researchers have explored the use of DNS analytics to detect VPN usage, as VPNs often require DNS resolution for establishing connections. By examining DNS queries and responses, it is possible to identify patterns associated with VPN connections, aiding in detection efforts. Additionally, some studies have investigated the use of passive monitoring and deep packet inspection (DPI) techniques for VPN user detection. DPI can analyze the contents of network packets, allowing researchers to examine payload data for signs of VPN usage. This approach can provide insights into the specific VPN protocols being used, further assisting in user identification(Raza *et al.* , 2022). Previous research on VPN user detection in a network has addressed the complexities of identifying and managing VPN connections. By leveraging behavioral analysis, traffic patterns, machine learning, DNS analysis, and other techniques, researchers have made significant strides in enhancing the ability to detect VPN users and gain insights into their activities. These advancements are crucial in maintaining network security, privacy, and effective network management in an environment where VPN usage is increasingly prevalent (Lavanya *et al.* , 2023). Below are reviews of work done by authors in the area of our research;

Aniss et al. , 2023, proposed a work on Characterizing the VPN Ecosystem in the Wild. In this paper, the researchers aimed to detect and characterize VPN servers in the wild, which facilitated the identification of VPN traffic. They conducted Internet-wide active measurements to locate VPN servers and analyzed their cryptographic certificates, vulnerabilities, locations, and fingerprints. The study identified 9.8 million VPN servers worldwide, utilizing various protocols, including OpenVPN, SSTP, PPTP, and IPsec. Vulnerability analysis revealed that SSTP was the most vulnerable protocol, with over 90% of detected servers susceptible to TLS downgrade attacks. Additionally, approximately 2% of the servers responding to VPN probes also responded to HTTP probes, classifying them as Web servers . Finally, the researchers used their list of VPN servers to identify VPN-related traffic within a large European ISP, finding that 2.6% of all traffic was associated with these VPN servers.

Lavanya et al. , 2023, proposed a work on Advances in Cybercrime Prediction: A Survey of Machine, Deep, Transfer, and Adaptive Learning Techniques. In this paper, the researchers aimed to provide a comprehensive survey of the latest advancements in cybercrime prediction using the mentioned techniques. They highlighted recent research related to each approach, reviewing over 150 research articles and discussing approximately 50 of the most recent and relevant ones. The review began by discussing common methods employed by cybercriminals and then shifted the focus to the latest machine learning and deep learning techniques, including recurrent and convolutional neural networks, known for their effectiveness in detecting

anomalous behavior and identifying potential threats. The paper also addressed transfer learning, which enables models trained on one dataset to be adapted for use with another dataset, and explored active and reinforcement learning as early-stage algorithmic research in cybercrime prediction. Additionally, the paper delved into critical innovations, identified research gaps, and outlined future research opportunities in the field of cybercrime prediction. Overall, the paper presented a holistic view of cutting-edge developments in cybercrime prediction, shedding light on the strengths and limitations of each method. It aimed to equip researchers and practitioners with essential insights, publicly available datasets, and the necessary resources to develop efficient cybercrime prediction systems.

Redha et al. , 2023, proposed a work on prisma-v2: Extension to Cloud Overlay Networks. In the paper, the researchers presented prisma-v2, an updated version of prisma, which served as a Packet Routing Simulator for Multi-Agent Reinforcement Learning. Prisma-v2 introduced several new features and enhancements. Firstly, it enabled the simulation of overlay network topologies by incorporating virtual links. Secondly, this release provided the capability to simulate control packets, improving the evaluation of network protocol overhead. Lastly, the researchers integrated the modules into a docker container, making it runnable on various machines and platforms.Prisma-v2 represented a significant advancement as it was the first realistic overlay network simulation playground available to the community. It offered the opportunity to test and assess new network protocols, contributing to the ongoing development and research in this field.

Nhien et al. , 2023, proposed a work on Darknet traffic classification and adversarial attacks using machine Learning. The research aimed to enhance darknet traffic detection by evaluating numerous machine learning and deep learning techniques for classifying such traffic and the associated application types. The study revealed that a Random Forest model exhibited superior performance compared to other state-of-the-art machine learning methods used in previous research with the CIC-Darknet2020 dataset. To assess the resilience of the Random Forest classifier, the researchers conducted experiments involving the obfuscation of select application type classes to replicate real-world adversarial attack scenarios. The findings demonstrated that even the best-performing classifier could be degraded by such attacks. The study also explored potential strategies for effectively addressing these adversarial attacks.

Faiz et al. ,2023, proposed a work on A deep learning-based framework to identify and characterise heterogeneous secure network traffic. In the paper, an effective deep learning-based framework was introduced, utilizing flow-time-based features for predicting heterogeneous secure network traffic. The study investigated state-of-the-art machine learning strategies, including C4.5, random forest, and K-nearest neighbor, for comparison purposes. The proposed 1D-CNN model outperformed the other machine learning techniques, achieving higher accuracy in classifying heterogeneous secure network traffic. Additionally, the deep learning model was employed to characterize major categories, such as virtual private network traffic, the onion router network traffic, and plain encrypted network traffic, into various application types. The experimental results demonstrated the effectiveness and feasibility of the proposed deep learning framework. It exhibited improved predictive capabilities when compared to state-of-the-art machine learning techniques commonly used for secure network traffic analysis.

Mohadmmed & Jan, 2023, proposed a work on A novel dataset for encrypted virtual private network traffic analysis. The primary objective of this research was to classify various network traffic patterns and encryption methods. However, it's worth noting that the authors did not provide insights into the specific methodology for detecting VPN users within the network.

Interestingly, the research did incorporate VPN data into its analysis, highlighting the relevance of understanding VPN usage patterns. A notable consideration arising from this work is the importance of developing a robust model for the detection of VPN users within a network. VPNs, while legitimate tools for secure communication, can potentially be exploited by malicious actors to gain unauthorized access to a network. Therefore, the absence of a dedicated model for VPN user detection represents a potential gap in the research landscape, warranting further investigation.
While the research made valuable contributions to the classification of network traffic and encryption behavior, it raised the pertinent issue of the need for a comprehensive model to detect VPN users within networks. Such a model could significantly enhance network security by identifying and mitigating potential threats associated with VPN usage.

3.0 Methodology

In this research, the K-Nearest Neighbor Algorithm is used to analyze and detect instances of Denial of Service attacks on a virtual private networks. To express the problem solving ability of KNN, we build its mathematical steps as seen below;

1. Data Representation:

Let X represent your feature dataset, where each row Xi corresponds to a set of feature values for a network traffic sample.
Let y represent the corresponding labels, where yi is the label (DoS attack or not) for the network traffic sample Xi (Anietie et al., 2022).

2. Distance Metric:

Choose a distance metric, typically Euclidean distance, to measure the similarity or dissimilarity between data points. The Euclidean distance between two data points Xi and Xj is given by:
d(Xi, Xj) = sqrt(sum((Xi,k - Xj,k)^2)) for k in [1, n]
where n is the number of features

3. Model Training:

Choose the value of k, the number of nearest neighbors to consider. This is a hyperparameter that you can tune through cross-validation.
Given a new data point Xnew for which you want to predict the label, find the k data points from the training set that are closest to Xnew based on the chosen distance metric.

4. Voting:

Among the k nearest neighbors, count how many belong to each class (DoS attack or not). Assign the class label to Xnew based on majority voting. That is, Xnew is classified as the class that occurs most frequently among its k nearest neighbors.
Mathematically, you can represent this as follows:
ŷnew = argmax(c, sum(I(yi = c) for i in NearestNeighbors(Xnew)))

where: ŷnew is the predicted label for the new data point Xnew.
c iterates over the possible classes (DoS attack or not).
NearestNeighbors(Xnew) represents the set of indices of the k nearest neighbors of Xnew.
I(yi = c) is an indicator function that returns 1 if yi is equal to class c, and 0 otherwise.
The k-NN algorithm is relatively simple but can be effective in many classification tasks. However, choosing an appropriate value for k and selecting the right features are critical steps in achieving good performance. You may also want to preprocess your data, such as normalizing feature values, before applying the k-NN algorithm.

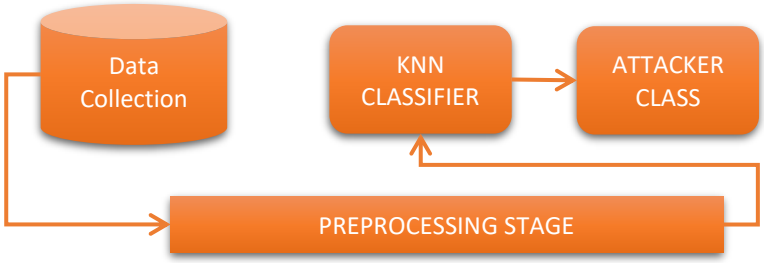

Fig.1.0 Block Diagram of the Proposed System

Figure 1.0 is the block diagram of the proposed system showing data flow from the data collect stage, to data preprocessing stage, to KNN classifier and finally to the outcome, which is the class.

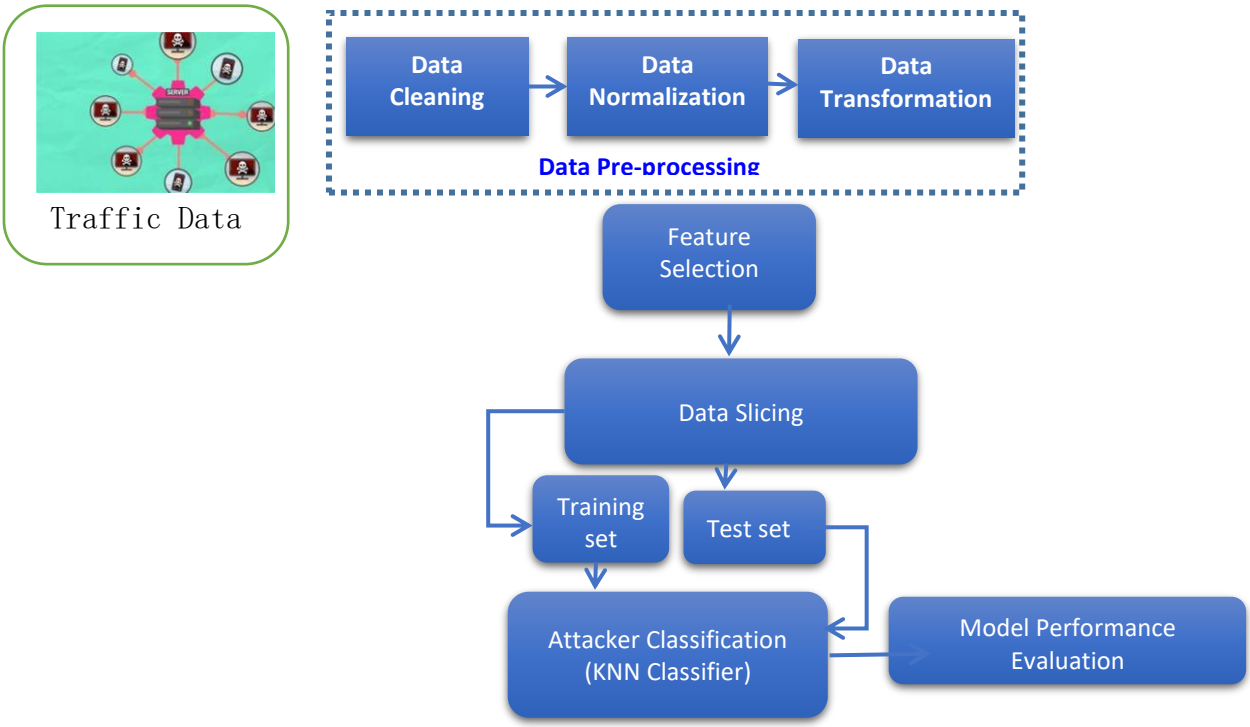

Fig.2.0 Conceptual Diagram of the Proposed System

Figure 2.0 represents the conceptual framework of the proposed system. This one is more detailed than the block diagram in figure 1.0. It brings out all the intricate stages from data collection to model classification and to the model performance evaluation.

3.0 RESULTS AND DISCUSSION

Table 1: Classification Report

	Precision	Recall	F1-Score	Support
0	1.00	0.80	0.89	2365
1	0.92	1.00	0.96	2674
Accuracy			0.94	5039
Macro avg	0.96	0.90	0.92	5039
Weighted avg	0.95	0.94	0.94	5039

Model Accuracy: 94%
In Table 1, the overall performance of the system is 94% indicating that the system is at its core in terms of performance on prediction of Denial of Service over a Virtual Private Network.

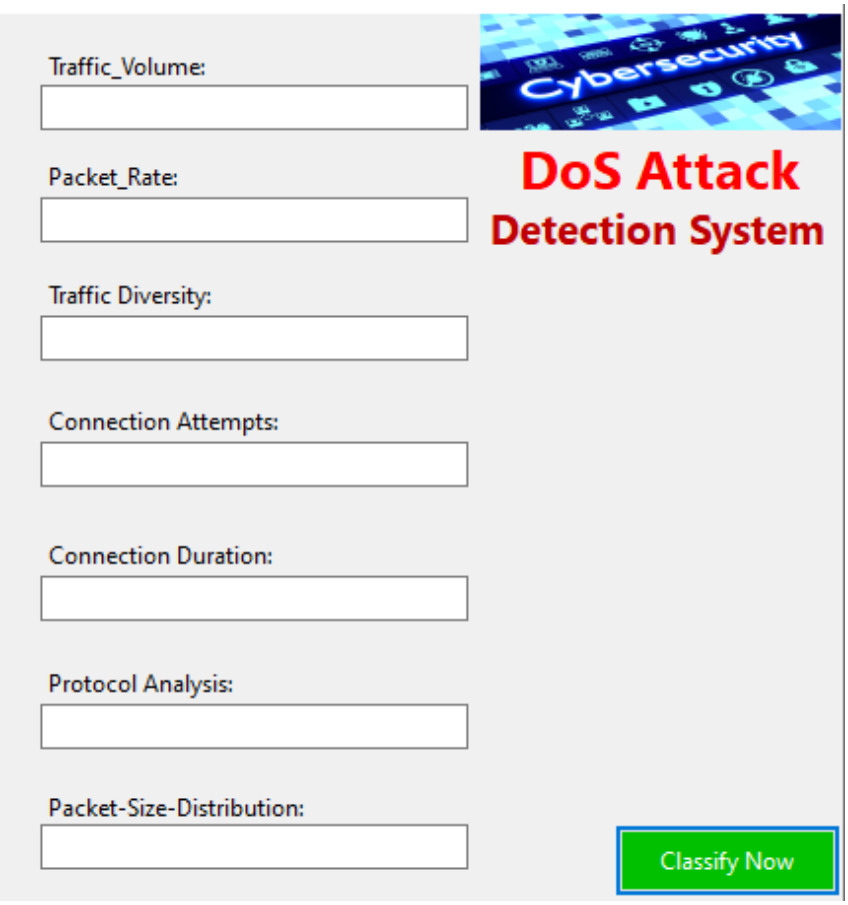

Fig. 3.0 Classification Interface

Figure 3.0 serves as the graphical user interface designed for the detection of Denial-of-Service (DoS) attacks on the VPN server. This interface allows users to input essential data features, namely Traffic-Volume, Packet-Rate, Traffic-Diversity, Connection-Attempts, Connection-Dur ation, Protocol-Analysis, and Packet-Size-Distribution. These carefully selected features are crucial inputs for the system to analyze and determine whether a given scenario constitutes a DoS attack or not.

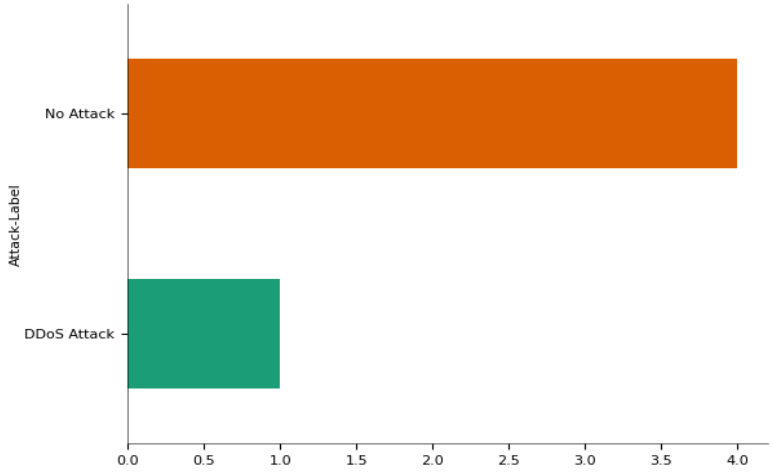

Fig. 4.0 Attack Label Distribution

In Figure 4.0, the distribution of Class labels is depicted, revealing a relatively low incidence of DoS attacks on the server. It is important to note that the presence of other types of attacks on the server is not discounted; however, our emphasis is specifically on DoS attacks. Consequently, the visualization indicates that the VPN server encountered a limited number of DoS attacks within the observed dataset**.**

5.0 Conclusion

In conclusion, our investigation into the detection of Denial-of-Service (DoS) attacks on a VPN server has provided valuable insights into the security space. Through the analysis of critical data features such as Traffic-Volume, Packet-Rate, Traffic-Diversity, Connection-Attempts, Connection-Duration, Protocol-Analysis, and Packet-Size-Distribution, our research has demonstrated a focused effort to pinpoint and understand the indicators associated with DoS attacks. The exploration of these features has enabled us to develop an effective interface, as illustrated in Figure 3.0, which serves as a dedicated tool for the detection of DoS attacks. Figure 4.0 further enhances our comprehension of the distribution of Class labels, affirming that while there is evidence of other attack types on the server, the concentration of DoS attacks is notably lower. This shows the significance of our tailored approach, concentrating on the specific characteristics indicative of DoS attacks. It is crucial to acknowledge that the observed low frequency of DoS attacks does not negate the possibility of other security threats. Instead, it emphasizes the need for a targeted focus on DoS detection within the broader context of server security. The utilization of advanced techniques such as K-Nearest Neighbors (KNN) classification, as demonstrated in our modeling, showcases the practical application of the identified data features for effective DoS attack identification. By combining the power of machine learning, our approach facilitates a proactive measure in fortifying the VPN server against potential disruptions. This not only enhances the security posture of the server but also contributes to the overall resilience of the network infrastructure.

REFERENCES

Maonan(2021). CENTIME: a direct comprehensive traffic features extraction for encrypted traffic classification, in: Proceedings of the 2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS), IEEE.

Ramos V, Suárez OJ, Suárez S, Febles VM, Aguirre E, Zradziński P, Rabassa LE, Celaya-Echarri M, Marina P, Karpowicz J, Falcone F, Hernández JA. (2022). Electromagnetic assessment of UHF-RFID devices in healthcare environment. Applied Sciences 12(20):10667 DOI 10.3390/app122010667.

Abugabah, A., Nizamuddin, N., & Abuqabbeh, A. (2020). A review of challenges and barriers implementing RFID technology in the healthcare sector. Procedia Computer Science, 170(3), 1003– 1010. DOI: 10.1016/j.procs.2020.03.094.

Sajogo M, Teoh SWK, Lebedevs T. (2023). Pharmacist clinical interventions: five years' experience of an efficient, low-cost, and future-proofed tool. Research in Social and Administrative Pharmacy 19(3):541–546 DOI 10.1016/j.sapharm.2022.12.008.

Ali, O., Ishak, M. K., & Bhatti, M. K. L. (2021). Emerging IoT domains, current standings and open research challenges: a review. PeerJ Computer Science, 7,(6), e659. DOI: 10.7717/peerj-cs.659.

Alliche, R. A., Da Silva Barros, T., Aparicio-Pardo, R., & Sassatelli, L. (2023). prisma-v2: Extension to Cloud Overlay Networks. Hal Open Access Science, 1-5.

Elluri, L., Mandalapu, V., Vyas, P., & Roy, N. (2023). Advances in Cybercrime Prediction: A Survey of Machine, Deep, Transfer, and Adaptive Learning Techniques. Journal Section, 1-28.

Islam, F. U., Liu, G., Liu, W., & ul Haq, Q. M. (2023). A deep learning-based framework to identify and characterise heterogeneous secure network traffic. IET Information Security, 17, 294–308.

Maghsoudlou, A., Vermeulen, L., Poese, I., & Gasser, O. (2023). Characterizing the VPN Ecosystem in the Wild. In Passive and Active Measurement Conference (pp. 21–23).

Naas, M., & Fesl, J. (2023). A novel dataset for encrypted virtual private network traffic analysis. Elsevier. DOI: 10.1016/j.dib.2023.108945.

Raza MA, Aziz S, Noreen M, Saeed A, Anjum I, Ahmed M, Raza SM. 2022. Artificial intelligence (AI) in pharmacy: an overview of innovations. INNOVATIONS in Pharmacy 12(2):13 DOI 10.24926/iip.v13i2.4839.

Roh H, Shin S, Han J, Lim S. 2021. A deep learning-based medication behaviormonitoring system. Mathematical Biosciences and Engineering 18(2):1513–1528 DOI 10.3934/mbe.2021078.

Schumann, Luca, et al. "Impact of evolving protocols and COVID-19 on internet traffic shares." arXiv preprint arXiv: 2201.00142 (2022).

Balasubramanian V, Vivekanandhan S, Mahadevan V. 2022. Pandemic tele-smart: a contactless tele-health system for effificient monitoring of remotely located COVID-19 quarantine wards in India using near-fifield communication and natural language processing system. Medical & Biological Engineering & Computing 60(1):61–79 DOI 10.1007/s11517-021-02456-1.

Diwen Xue, et al., {OpenVPN} is open to {VPN} fingerprinting, in: Proceedings of the 31st USENIX Security Symposium (USENIX Security 22), 2022.

Sriboonruang P, Rattanamahattan M. 2022. Barcode scanning technology to improve predispensing errors. Greater Mekong Subregion Medical Journal 3(1):7–12.

Villegas-Ch W, García-Ortiz J, Román-Cañizares M, Sánchez-Viteri S. 2021. Proposal of a remote education model with the integration of an ICT architecture to improve learning management. PeerJ Computer Science 7(3):e781 DOI 10.7717/peerj-cs.781.

Waleed Afandi, et al., Fingerprinting technique for you tube videos identification in network traffic, IEEE Access 10 76731–76741.

Abugabah A, Nizamuddin N, Abuqabbeh A. 2020. A review of challenges and barriers implementing RFID technology in the healthcare sector. Procedia Computer Science 170(3):1003–1010 DOI 10.1016/j.procs.2020.03.094.

Vagaš M, Galajdová A, Šimšík D, Onofrejová D. 2019. Wireless data acquisition from automated workplaces based on RFID technology. IFAC-PapersOnLine 52(27):299–304 DOI 10.1016/j.ifacol.2019.12.677.

Rust-Nguyen, N., Sharma, S., & Stamp, M. (2023). Darknet traffic classification and adversarial attacks using machine learning. Journal of Computers and Security, 123(2), 1-17.

Aniss M., Lukas V., Ingmar P., Oliver . (2023). Characterizing the VPN Ecosystem in the Wild. https://doi.org/10.48550/arXiv.2302.06566

Elluri, L., Mandalapu, V. , Vyas, P., Roy, N. (2023). Advances in Cybercrime Prediction: A Survey of Machine, Deep, Transfer, and Adaptive Learning Techniques.

Nhien R., Shruti S., Mark S.(2023). Darknet traffic classification and adversarial attacks using machine learning. Journal of Computers and Security, 127(2023). https://doi.org/10.1016/j.cose.2023.103098

Faiz U. I., Guangjie L., Weiwei L.(2022). A deep learning-based framework to identify and characterise heterogeneous secure network traffic.IET information Security, 17(2), 294-308.

Naas M, Fesl J. (2023). A novel dataset for encrypted virtual private network traffic analysis. Data Brief. 2023 Feb 1;47:108945. doi: 10.1016/j.dib.2023.108945.

Edet, A. E. and Ansa, G. O. (2023). Machine learning enabled system for intelligent classification of host-based intrusion severity. Global Journal of Engineering and Technology Advances,16(03), 041–050.

Ekong, B., Ekong, O., Silas, A., Edet, A., & William, B. (2023). Machine Learning Approach for Classification of Sickle Cell Anemia in Teenagers Based on Bayesian Network. Journal of Information Systems and Informatics, 5(4), 1793-1808. https://doi.org/10.51519/journalisi.v5i4.629.

Anietie Ekong, Blessing Ekong and Anthony Edet (2022), Supervised Machine Learning Model for EffectiveClassification of Patients with Covid-19 Symptoms Based on Bayesian Belief Network, Researchers Journal ofScience and Technology(2022),2, pp-27-33.

Uwah, A. and Edet, A. (2024).Customized Web Application for Addressing Language ModelMisalignment through Reinforcement Learning from HumanFeedback. World Journal of Innovation And Modern Technology,8,(1), 62-71. DOI: 10.56201/wjimt.v8.no1.2024.pg62.71.

Edet, A., Ekong, B. and Attih, I. (2024). Machine Learning Enabled System for Health Impact Assessment of Soft Drink Consumption Using Ensemble Learning Technique. INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND MATHEMATICAL THEORY,10(1):79-101, DOI: 10.56201/ijcsmt.v10.no1.2024.pg79.101

I. J Umoren & S. J. Inyang (2021) “Methodical Performance Modelling of Mobile Broadband Networks with Soft Computing Model,” International Journal of Computer Applications, vol. 174, no. 25, pp. 7-21.

S. Inyang and I. Umoren (2023) "From Text to Insights: NLP-Driven Classification of Infectious Diseases Based on Ecological Risk Factors," Journal of Innovation Information Technology and Application (JINITA), vol. 5, no. 2, pp. 154-165,

S. Inyang and I. Umoren (2023) “Semantic-Based Natural Language Processing for Classification of Infectious Diseases Based on Ecological Factors,”. International Journal of Innovative Research in Sciences and Engineering