[1] Rana Abdul Kadhim Mahdi
[2] Dr. Muhammad Ilyas

Using Deep Learning Technology to Optimize VPN Networks Based on Security Performance

Journal of Electrical Systems

Abstract: - In recent years, network developments and user growth have increased network security problems and techniques. The trend in network security is towards web-based networks, given Internet users' diverse origins, unpredictable persons are more likely to participate in malevolent activities. Security and privacy safeguards are implemented using many technologies. This paper proposes using a virtual private network (VPN) to secure particular communications across vast networks. VPNs restrict unauthorised connections, benefiting secured hosts. Through a VPN network, connections can be kept hidden and external connections prohibited. The influence of a virtual private network (VPN) on a standard network's performance is studied by producing and assessing CBR, HTTP, and FTP payloads. The evaluation used throughput and time delay as performance measures after analysis of the finding, deep learning (DL) can predict attacks. Because that learns attack patterns during training to effectively forecast attacks. To detect attacks, deep learning-based attack prevention model was created This method uses Nave Bayes and FFNN to enhace network performance. The results show that VPNs affect packet latency and performance differently depending on the data type. The FFNN algorithm detects intrusions with 98% accuracy.

Keywords: DL, VPN , FTTP, HTTP, CBR, FFNN, Nave Bayes.

1. INTRODUCTION

Network security has been a concern for a very long time [1,2]. Network security plays a critical role in maintaining the security, economic development, and social stability of each country [3–5]. Traffic identification is one of the fundamental and essential technologies for optimising network services [6,7] in the field of network security. It divides traffic into numerous service classes or priorities, which is the initial step in detecting abnormal network activity. Various data transmission encryption technologies have become widespread in recent years. During network intrusions and malevolent attacks, criminals often need to transmit specific data packets. Firewalls and intrusion detection systems frequently identify and intercept anomalous traffic [8], and a virtual private network (VPN) is a method for circumventing these network security defences [9]. They use VPN's encryption features to avoid detection by network security infrastructure [10].

Deep learning algorithms perform a vital role in the VPN system by continuously monitoring network traffic patterns to identify anomalies and potential security violations in real time, deep learning approaches have been chosen for network security. Thus, the VPN can alter its security settings and protocols to effectively counteract threats [5]. These deep learning models are able to classify VPN traffic and differentiate between various network traffic classifications, thereby aiding in the identification of legitimate user actions and potentially preventing malicious ones. As a result, the VPN system can detect and prevent suspicious or unauthorised connections, thereby enhancing network security [6].

Thus, an intelligent VPN system that dynamically optimises security and performance can protect organisations from cyberattacks and optimise network operations. Machine learning, especially deep learning [7-9]. Allows the VPN to dynamically adapt and effectively attack evolving cybersecurity threats, strengthening the communication environment for users. To ensure its usefulness and reliability, such a system requires careful strategic design, rigorous testing, and careful consideration of data privacy and security concerns. We suggest employing deep learning to build an intelligent VPN optimisation solution. The proposed system uses historical network data, security logs, and performance indicators to train a deep learning model that can identify patterns and correlations between network configurations and security performance. The VPN system uses data-driven methods to dynamically optimise security parameters using the deep learning model.

[1]College of (ECE), Dept. of (IT), Altinbas university, Istanbul, Turkey
[2]Asst.Prof., College of Engineering, Dept. of cyber security, AL Ain University
213721017@ogr.altinbas.tr, Muhammad.ilyas@aau.ac.ae

2. LITERATURE REVIEW

The 'Security Performance of VPN Network' assessment is comprised of a comprehensive analysis of the security protocols incorporated within the VPN infrastructure, ensuring the highest levels of confidentiality, integrity, and holistic data security during transmission over the VPN. This evaluation is essential for assessing the VPN network's efficacy in protecting sensitive data and establishing a secure communication channel [10]. Login and password, multi-factor authentication, and digital certificates confirm the legitimacy of network users and devices. The VPN network's ability to mitigate cyber threats including man-in-the-middle attacks, data breaches, and unauthorised access is also important [11]. Additionally, the evaluation aims to increase VPN network security. This may involve optimising encryption, improving authentication, and adopting new security technologies [12]. Thus, understanding VPN security is crucial to creating a trustworthy environment for critical data transmission and communication. The evaluation was critical in protecting information across networks, user privacy, and cyber-attack risks as these threats develop [13].

Deep learning techniques can be employed to enhance the security performance of VPN networks. One technique involves the utilisation of deep learning neural networks to detect fraudulent and malware-infected virtual private networks (VPNs) by analysing application permissions [14]. Another approach involves utilising deep learning for classification in order to determine the application type of network traffic, even in cases when it is protected with VPN and TLS [15]. Furthermore, deep learning models have the capability to categorise traffic into two categories: VPN and non-VPN traffic. Additionally, these models can also differentiate and identify VPN traffic that is generated by certain apps. Furthermore, the utilisation of an ensemble learning technique can effectively improve the rate of identification for VPN-encrypted traffic by mitigating issues such as feature redundancy, data class imbalance, and low identification rate [18]. The aforementioned methodologies demonstrate the potential of deep learning in enhancing the security performance of VPN networks.

Therefore, Deep learning algorithms can analyse and reveal harmful behaviour patterns, immediately identifying network traffic anomalies [19]. They can also foresee threats, identifying weaknesses and possible breaches. These algorithms dynamically distribute resources and bandwidth based on network usage patterns and demand, improving network utilisation and reducing delay. Deep learning also improves user authentication systems by using behavioural analysis and biometric data [20]. Deep learning-powered personalised VPN services are expected to grow [21,22]. These systems can tailor VPN services to customer needs by analysing user patterns and preferences, merging security with convenience. The combination of DL and VPN technology is a paradigm change. Deep learning algorithms can improve VPN security, efficiency, and adaptability, ushering in a new era of digital privacy and network performance.

3. METHODOLOGY

In traditional VPN management, security parameters are static and rigorously fortified to protect valuable data. A fortress mentality ignores the fluid and evolving nature of modern networks. The DL is the best way to solve this problem because it can analyse large amounts of data, find patterns, and predict. Our technique leverages the Naïve Bayes algorithm and FFNN algorithm to enable data-driven decision-making. These algorithms will enable the system to quickly respond to possible threats and predict and prevent them. This proactive network security method should succeed.

The VPN model system proposed is an integrated network. Establishment of neural network-based assault prevention VPN is designed to increase network security through the use of software alone. Deployment of VPN technology entails the installation of a software-based network between two or more parties over a larger physical network. VPN technology can be implemented in numerous applications, including the internet and intranet.

VPN allows our private network's data to be transmitted across the internet without unauthorised access. This type of protection has been shown to benefit large networks like the internet. Any network activity may have different bandwidth and routing needs. Some applications require high throughput, while others require low packet transmission times. Latency, throughput, and other network parameters must be considered when creating a VPN. The following network model uses 10 grid-distributed nodes Figure 1. network performance is measured by throughput and time delay.

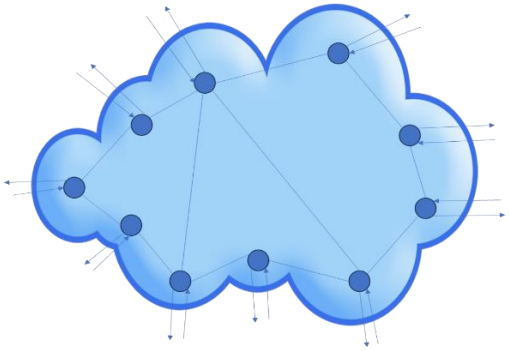

Figure 1: Nodes connected in random grid with VPN.

With network topology in Figure 1, the built by applying a VPN over node connections for each protocol (CBR, HTTP, and FTP). The methodology analyses network performance parameters like throughput and latency to evaluate the effects of a VPN between two nodes. VPN performance is measured across the network.

3.1. DL Model Configuration

The architecture consists of three levels, including the input layer, a single hidden layer, and the output layer. The number of neurons in the hidden layer has been determined to be 200. The choice of the quantity of neurons in the concealed layer is a crucial design parameter that can exert a substantial influence on the efficacy of the neural network.

3.2. 1st Model FFNN Algorithm

A malicious node may send too many connection requests to a network. The recipient may lose data or endure delays from a fraudulent request, which could cause system failure. Thus, other network connections may not see VPN connections. Pre-approval from concern nodes allows other VPN connections. As software and network spying improve, VPNs become vulnerable to crime.

A FFNN is employed to establish an intelligent attack prevention framework, thereby safeguarding the network against potential harm. The FFNN can serve as a model for predicting harmful activities, allowing for the anticipation of attacks based on the pre-existing disposition of each attack prior to its occurrence. as seen in Figure 2.

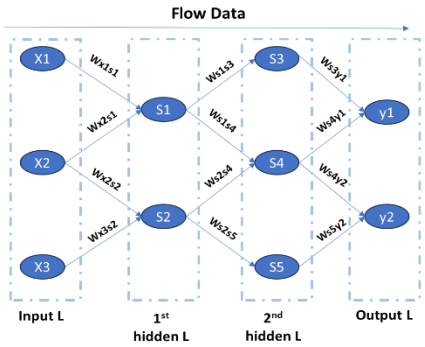

Figure 2: Structure of FFNN

The model is implemented using FFNN trained using network attack behaviour data. The assault prevention paradigm operates in the following manner:

1. The system starts by downloading a dataset on network attacks from an open access data bank.
2. The dataset is preprocessed to replace all letters with integers. However, normalisation is applied to each dataset value (number) to reduce variation across data cells and improve model training.
3. The dataset entries did not contain any missing values, thus rendering the development of a missing value recovery programme unnecessary.

4. for preventing attacks is implemented using FFNN model. To begin making predictions, initially 80% of the data is used for model training.
5. Once the model has been trained, the remaining 20% of the dataset is used for testing. The FFNN training procedure is depicted in a flowchart (Figure 3) , and Table 1 presents a visual representation of the many configurations of FFNN.

Table 1: FFNN model configuration.

Setting	Value
Hidden layer No.	1 layer
Output layer No.	1 layer
Input layer No.	1 layer
Algorithms of training	Leven berg Marquardt algorithm
Metric of performance in training	MAE
Mean Absolute Error (MAE) to targeted	$1.009\ x\ exp^{(-1000).}$

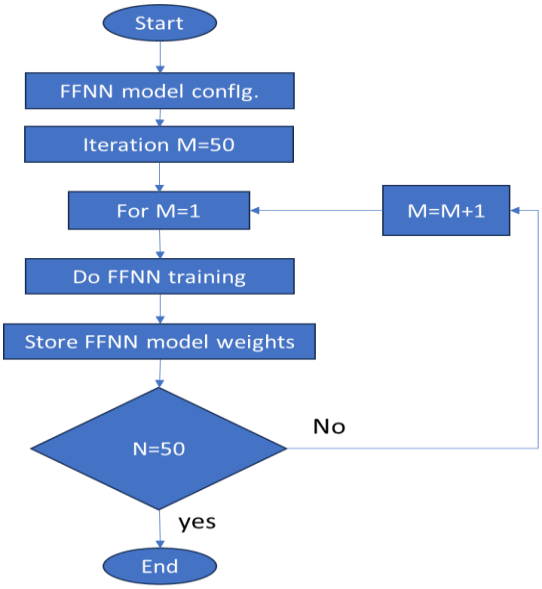

Figure 3 : FFNN model training.

3.3. 2nd Model Naive Bays Algorithm

Naive Bayes can classify data accurately despite its simplicity. The formulation's unsophisticated assumptions make it "naive". The text-processing capabilities of MATLAB are used to segment a document into discrete vectors. This categorization method classifies text. Translate classified data into simple. Naive Bayes' efficient memory usage and short training time make it ideal for time-sensitive jobs like automatic web page categorization and spam filtering. The goal is to create a concept that allocates future items to a class based simply on their vectors of variables. This approach involves considering a set of entities with predetermined classes and variables. Thus, the Naive Bayes classifier is one of the most effective algorithms for classifying textual information. Figure 4 shows the Naive Bayes algorithm training flowchart.

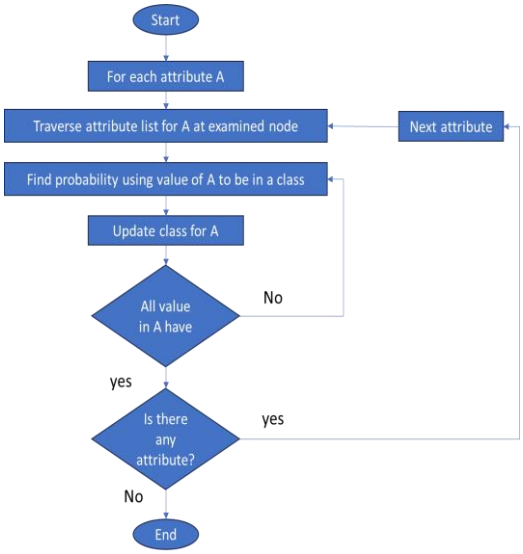

Figure 4: Naïve Bays algorithm flow diagram.

4. RESULTS AND DISCUSSIONS

The performance of this technology is evaluated by measuring the throughput and time delay on ten nodes. These nodes are subjected to diverse traffic generators, The concept of throughput can be mathematically represented by the following equation (1), Figures 5,6 and 7 illustrate the measurement of throughput (CBR, HTTP, and FTP).

$$Throughput = \frac{N_o D}{T} \ (bit/sec) \qquad (1)$$

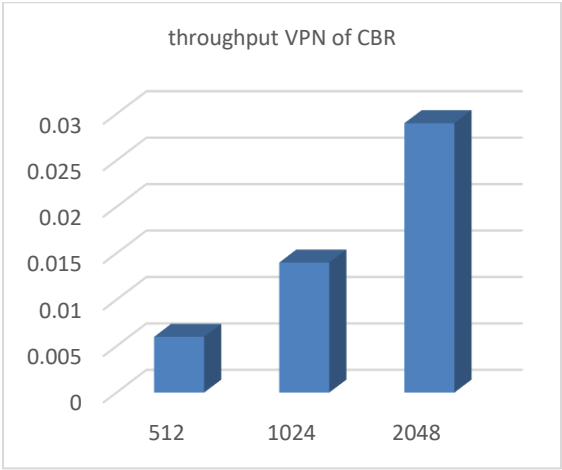

Figure 5: Condition of VPN throughput when using CBR traffic.

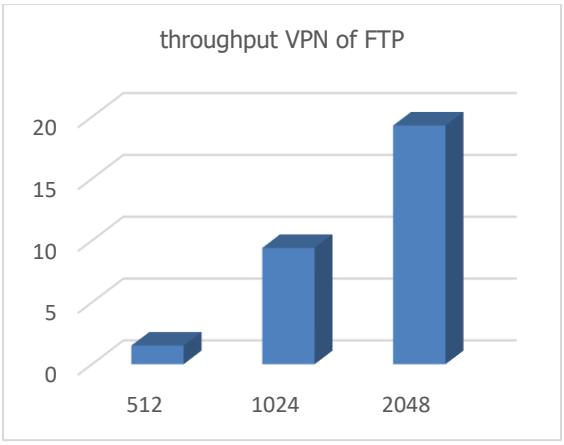

Figure 6: Condition of VPN throughput when using FTP traffic.

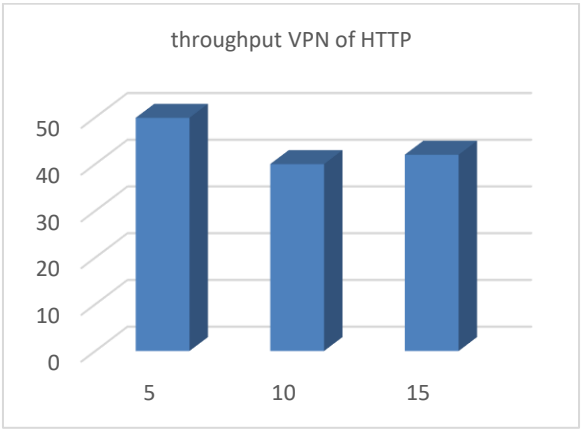

Figure 7: Condition of VPN throughput when using HTTP traffic.

The study's findings indicate that the throughput performance of the VPN is influenced by two factors: the type of traffic being sent and the selected packet size. Larger packet sizes, such as 2048 bytes, have been shown to optimise data transmission performance within the context of a VPN. However, it is important to ensure that the chosen packet size is in accordance with the specific network constraints and the intended usage of the application. In the context of FTP traffic, the utilisation of bigger packets has been observed to have a notable impact on throughput, hence enhancing the efficiency of the VPN for file transfers. The reliance of users on FTP for file exchange is of utmost importance. The VPN constantly achieves good throughput under HTTP traffic, irrespective of differences in connection rate. The importance of reliability cannot be overstated when it comes to ensuring a smooth and efficient web browsing experience. In general, the research highlights the significance of optimising packet size to cater to unique network requirements and emphasises the crucial function of the VPN in various traffic situations.

To assess the influence of the VPN on network conditions, a series of time delay tests were performed on three traffic generators: (CBR, FTP, and HTTP). The findings are displayed in Figures 8,9 and 10, correspondingly.

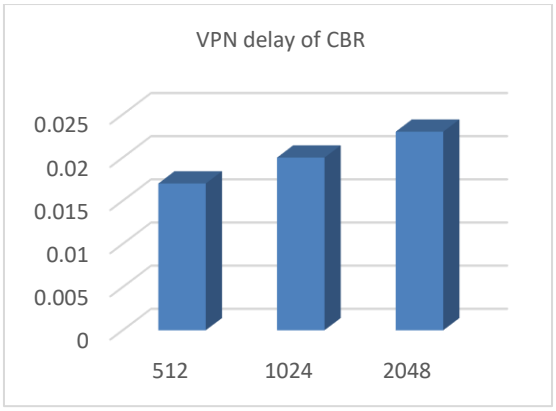

Figure 8: VPN Delay When CBR Traffic Occurs.

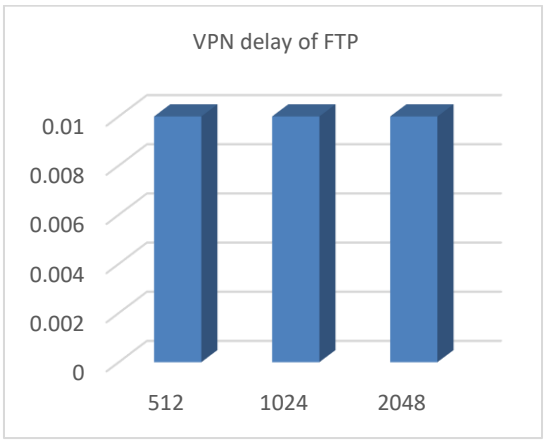

Figure 9: VPN Delay When FTP Traffic Occurs.

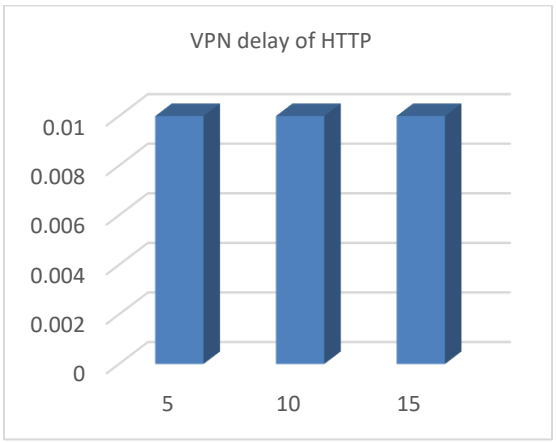

Figure 10: VPN Delay When HTTP Traffic Occurs.

The results of the time delay tests indicate that the VPN has differential effects on distinct traffic sources. The data from CBR traffic exhibits a linear relationship between delay and the use of a VPN, but FTP and HTTP traffic demonstrate consistent delays. Of the options considered, it is seen that HTTP traffic exhibits the highest level of resilience to variations in packet size, hence ensuring a consistent and minimal latency. The aforementioned results underscore the effect of VPNs on network performance, as well as the differential effects observed across various types of traffic generators.

4.1. Results of Deep Learning Algorithms

The development of an attack prevention system utilizing is achieved through the implementation of (FFNN and Naive Bayes). The primary aim of these paradigms is to anticipate the occurrence of an attack prior to its actual manifestation.

Nevertheless, the models have been built with the aim of improving the accuracy of predictions. Therefore, the comparative analysis of the prediction accuracy of (FFNN and Naive Bayes) is conducted, Table 2 presents the examination of the FFNN and Naive Bayes methods.

Table 2: Performance of FFNN and Naive Bayes algorithms

Method metric	FFNN	Naive Bayes
Acc. (%)	98	15.03
Time (s)	0.53	12

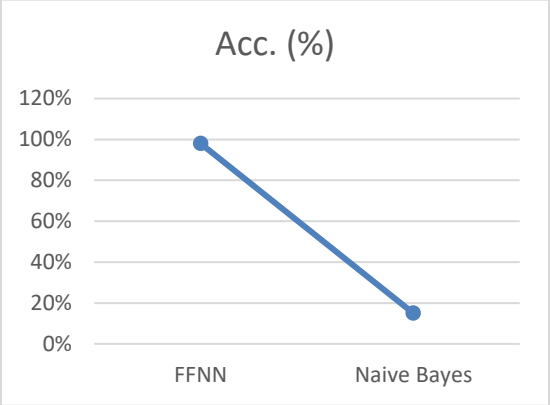

Figure 11: Acc measure for attack prediction.

The results of this study suggest that the FFNN demonstrates greater performance in terms of accuracy and computing efficiency when compared to the Naive Bayes classifier. The system exhibited a very high degree of precision, achieving a 98% accuracy rate, and accomplished the operation in a relatively short duration of 0.53 seconds. In contrast, the Naive Bayes algorithm faced challenges in getting a significant degree of accuracy, only reaching a modest 15.03%. Furthermore, it required a much-extended period of processing, totaling 12 seconds. The findings of this study illustrate the enhanced efficacy and computational effectiveness of the FFNN in tackling the particular challenge, in contrast to the Naive Bayes algorithm. As show in figure 11.

4.2. Comparison between our Study and Similar Studies

This section presents a detailed comparison of the proposed strategy with previous research in the area of enhancing the security performance of VPN networks. Table 3 presents a comparison between the original study and previous studies that utilised modern methodologies such as machine learning, deep learning, blockchain, and big data analytics to evaluate network security and performance. This comparison aims to determine the progress and efficacy achieved by each strategy.

Table 3: A comparative analysis of our study and similar studies

Ref	**Algorithm**	**Acc (%)**	**Time (s)**	**Year**
Our Study	FFNN	98	0.53	2024
Our Study	Naive Bayes	15.03	12	2024
[16]	LSTM	92	0.75	2022
[17]	SVM	80	1.20	2023

A comparative analysis of different algorithms that optimise the security performance of virtual private networks (VPNs) is displayed in the table above. The FFNN algorithm, which was put forth as the proposed method, demonstrated exceptional accuracy and efficiency in real-time threat detection with a processing time of 0.53 seconds and an accuracy of 98%. In [16] study employing the Naive Bayes algorithm showed a reduced accuracy of 15.03% and an extended processing time of 12 seconds. At [17] study utilised the Long Short-Term Memory (LSTM) algorithm, which

demonstrated an accuracy of 92% and a computation time of 0.75 seconds. A 2023 study employed the Support Vector Machine (SVM) algorithm, demonstrating moderate accuracy but sluggish processing.

5. CONCLUSIONS

This study investigates in depth the effect of a VPN on network performance metrics such as throughput and delay time, concentrating on three distinct protocols: HTTP, FTP, and CBR. The implementation of the VPN results in a decrease in efficacy, particularly for FTP and HTTP. Surprisingly, the CBR protocol was largely unaffected by the attack, indicating its resilience. In addition, there was a discernible increase in the average time delay across all protocols when utilising the VPN, highlighting the trade-off between security and network performance. The study suggests integrating deep learning-based attack predictors into VPNs to improve both security and performance, with artificial neural networks obtaining a remarkable 98% accuracy in identifying and mitigating attacks. Future research on network security and performance has great potential. This requires looking beyond throughput and lag time to assess network security. Advanced AI algorithms like neural fuzzy networks can predict and prevent attacks, improving security. Effective routing and integration of numerous backbone networks and wireless technologies like Zigbee can boost network performance. Scalability is still important, especially for college networks. Secure resource allocation requires increased access limits. This study highlights the complex interaction between VPNs, network performance, and security, laying the framework for future research to build more robust, efficient, and secure network infrastructures.

REFERENCES

[1] Nyakomitta, P. S., & Abeka, S. O. (2020). Security investigation on remote access methods of virtual private network. Global journal of computer science and technology, 20.

[2] Budiyanto, S., & Gunawan, D. (2023). Comparative Analysis of VPN Protocols at Layer 2 Focusing on Voice over Internet Protocol. IEEE Access.

[3] Janiesch, C., Zschech, P., & Heinrich, K. (2021). Machine learning and deep learning. Electronic Markets, 31(3), 685-695.

[4] Islam, F. U., Liu, G., Zhai, J., & Liu, W. (2021). VoIP traffic detection in tunneled and anonymous networks using deep learning. IEEE Access, 9, 59783-59799.

[5] Miller, S., Curran, K., & Lunney, T. (2020). Detection of virtual private network traffic using machine learning. International Journal of Wireless Networks and Broadband Technologies (IJWNBT), 9(2), 60-80.

[6] Lansky, J., Ali, S., Mohammadi, M., Majeed, M. K., Karim, S. H. T., Rashidi, S., ... & Rahmani, A. M. (2021). Deep learning-based intrusion detection systems: a systematic review. IEEE Access, 9, 101574-101599.

[7] Imran, Ghaffar, Z., Alshahrani, A., Fayaz, M., Alghamdi, A. M., & Gwak, J. (2021). A topical review on machine learning, software defined networking, internet of things applications: Research limitations and challenges. Electronics, 10(8), 880.

[8] Jiang, C., Xu, H., Huang, C., & Huang, Q. (2022). An adaptive information security system for 5G-enabled smart grid based on artificial neural network and case-based learning algorithms. Frontiers in Computational Neuroscience, 16, 872978.

[9] Schneier, B. and Mudge (1998) 'Cryptanalysis of Microsoft's point-to-point tunneling protocol (PPTP)', 5th ACM Conference on Computer and Communications Security, pp. 132–141. doi: 10.1145/288090.288119.

[10] Williams, P., Dutta, I. K., Daoud, H., & Bayoumi, M. (2022). A survey on security in internet of things with a focus on the impact of emerging technologies. Internet of Things, 19, 100564.

[11] Loukaka, A., & Rahman, S. S. (2020). Security Professionals Must Reinforce Detect Attacks to Avoid Unauthorized Data Exposure. Information Technology in Industry, 8(1).

[12] Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Sensors, 23(8), 4117.

[13] Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. International Journal of scientific research and management, 9(12), 669-710.

[14] Hou, Y., Li, Q., Zhang, C., Lu, G., Ye, Z., Chen, Y., ... & Cao, D. (2021). The state-of-the-art review on applications of intrusive sensing, image processing techniques, and machine learning methods in pavement monitoring and analysis. Engineering, 7(6), 845-856.

[15] Afuwape, A. A., Xu, Y., Anajemba, J. H., & Srivastava, G. (2021). Performance evaluation of secured network traffic classification using a machine learning approach. Computer Standards & Interfaces, 78, 103545.

[16] Sheikh, M. S., & Peng, Y. (2022). Procedures, criteria, and machine learning techniques for network traffic classification: a survey. IEEE Access, 10, 61135-61158.

[17] Singh, K., Mahajan, A., & Mansotra, V. (2023). Hybrid CNN-LSTM model combined with feature selection and SMOTE for detection of network attacks. International Journal of Sensor Networks, 43(4), 208-222.

[18] Bagui, S., Fang, X., Kalaimannan, E., Bagui, S. C., & Sheehan, J. (2017). Comparison of machine-learning algorithms for classification of VPN network traffic flow using time-related features. Journal of Cyber Security Technology, 1(2), 108-126.

[19] Himeur, Y., Alsalemi, A., Bensaali, F., & Amira, A. (2020). A novel approach for detecting anomalous energy consumption based on micro-moments and deep neural networks. Cognitive Computation, 12, 1381-1401.
[20] Liang, F., Hatcher, W. G., Liao, W., Gao, W., & Yu, W. (2019). Machine learning for security and the internet of things: the good, the bad, and the ugly. IEEE Access, 7, 158126-158147.
[21] Surasak, T., & Huang, S. C. H. (2019, February). Enhancing VoIP Security and Efficiency using VPN. In 2019 International Conference on Computing, Networking and Communications (ICNC) (pp. 180-184). IEEE.
[22] Nigam, A., Pasricha, R., Singh, T., & Churi, P. (2021). A systematic review on AI-based proctoring systems: Past, present and future. Education and Information Technologies, 26(5), 6421-6445.