IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

The Impact of Artificial Intelligence on Strengthening Cybersecurity Protocols

Kundan Kumar Mishra[1] and Dr. Amaravatid Pentaganti[2]
Research Scholar, Department of Computer Science and Engineering[1]
Supervisor, Department of Computer Science and Engineering[2]
NIILM University, Kaithal, Haryana, India

Abstract: *To protect vital assets and data, cutting-edge intrusion detection systems (IDS) are required due to the increasing complexity of cyberattacks. The goal of the project is to investigate how Artificial Intelligence (AI) may improve the capacity of the Intrusion Detection System (IDS) to recognise and categorise network traffic and spot unusual activity. This article provides a brief introduction to IDS and AI, reviews the research, and emphasises the need of using sophisticated language models to improve cybersecurity. The study describes the approach used to evaluate AI's effectiveness in IDS. In order to provide a thorough assessment, the research also takes into account important performance indicators including reaction speed, false positive rate, and detection accuracy. Results show that artificial intelligence (AI) may significantly improve the accuracy of AI in identifying and thwarting cyberattacks. However, the research also highlights certain drawbacks and difficulties with integrating AI into IDS, namely computational cost and possible biases in training data. In addition to highlighting the potential of complex language models like ChatGPT to enhance cybersecurity solutions, this study provides insights into resolving related issues for a more resilient and successful defence against sophisticated cyberattacks.*

Keywords: Intrusion Detection Systems, Cybersecurity, AI

I. INTRODUCTION

Intrusion Detection Systems (IDS) are essential security measures that protect network infrastructures from malicious activities and unauthorised access by detecting them. They have made significant strides since their introduction in the middle of the 1980s in order to keep up with the increasing complexity of crimes using computers [1]. Network intrusion detection and prevention (NIDS) and heuristic behavioural analysis (IPS) systems are subsets of intrusion detection systems (IDS) that use statistical anomaly detection, signature analysis, and network traffic analysis to look for indications of hostile activity [2]. These systems possess the capacity to detect and maybe prevent unwanted activities and assaults that traditional security measures like firewalls could overlook [3].

With more sophisticated threats aiming to damage the confidentiality, integrity, and availability of network systems, it is critical that cyberattack detection and response become more accurate. Pietraszek estimates that 99% of intrusion detection signals have nothing to do with cybersecurity issues since routine and malicious activity very slightly differs from one another [4]. Scholars have put forward a number of methods to improve IDS capabilities, including support vector machines (SVMs) [2], fuzzy logic [1], and neural networks (NNs). These methods have shown potential in decreasing false positives and raising detection rates for various attack kinds, including as denial-of-service (DDoS) assaults [2].

Given that ChatGPT and related AI models may make use of machine learning and natural language processing methods to comprehend intricate patterns and behaviours in network traffic, there is interest in the potential for these models to improve intrusion detection capabilities. It might be feasible to enhance the identification of complex assaults, lower false positives, and provide more effective reaction mechanisms by incorporating AI models into IDS. IDS may enhance the detection of complex assaults, lower false positives, and allow more effective response mechanisms by using ChatGPT or comparable AI models. This study investigates ChatGPT's potential to raise IDS's accuracy and improve its cybersecurity capabilities.

DOI: 10.48175/568

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

Background

In the late 1980s, intrusion detection systems became a crucial part of cybersecurity. Since then, the industry has quickly changed to meet the increasing complexity and diversity of cyberthreats. Large, centralised mainframe systems were the primary target of early intrusion detection systems (IDSs); but, as computer networks proliferated, IDSs grew to safeguard these increasingly linked systems.

Traditional Methods of Intrusion Detection Systems

Anomaly-based detection (AD) and signature-based detection (SD) make up traditional IDS [5]. A technique called signature detection (SD) finds patterns or sequences in network data that correspond to known threat signatures. This method has a low false positive rate for known assaults and is very successful in identifying them [5]. However, this technique has a disadvantage in that it may not be able to identify new or undiscovered dangers. Furthermore, to guarantee the effectiveness of the SD system, the signature database must be updated on a regular basis.

An approach called anomaly-based detection (AD) scans network data for patterns that deviate from expected behaviour and may point to a possible assault [5]. AD uses statistical analysis, machine learning algorithms, and other techniques to create a baseline of typical behaviour and spot abnormalities. This method is flexible enough to adjust to changing network conditions and is capable of identifying unknown or unusual assaults. But compared to Signature Detection (SD), AD has a larger false positive rate, and it needs some training to set up a baseline of typical behaviour. The high false positive and low false negative rates linked to AD may be addressed using a mixed strategy.

Overview of AI-based IDS

The purpose of intrusion detection systems (IDS), which are crucial parts of contemporary network security architecture, is to identify and stop assaults, abuse, and unauthorised access to computer systems and networks [13]. Conventional intrusion detection systems use rule- and signature-based techniques to identify known threats. Nonetheless, these conventional methods are finding it more and more challenging to keep up with the quick spread of cutting-edge and unique attack methods as the cyber threat environment changes [14]. A promising approach to addressing these issues is artificial intelligence (AI)-based intrusion detection systems (IDS), which make use of machine learning and other AI techniques. These systems offer a number of advantages over conventional methods, including adaptability, pattern recognition, and real-time detection and response capabilities [13].

Advantages of AI-based IDS over Traditional Methods

The intrinsic flexibility of AI-based IDS is one of its main benefits. While AI-based IDS may eventually learn and adapt to new threats and changing network behaviour, conventional IDS depend on a predetermined set of signatures and rules to identify known threats. As a result, they may identify assaults and abnormalities that were previously unknown, providing a stronger and more proactive defence against cyberthreats that are always changing.

Pattern Recognition

Using machine learning algorithms, these systems can effectively identify patterns indicative of malicious activity even in the absence of a known attack vector or method. This feature of AI-based intrusion detection systems (IDS) enables them to detect a wide range of threats, including advanced persistent threats (APTs) and zero-day attacks, which are frequently missed by traditional signature-based IDS [15]. Recognising patterns in large volumes of network data is another advantage of AI-based IDS.

Real-time Detection and Response

Real-time detection and response capabilities are another area where AI-based IDS excels.

AI-based intrusion detection systems (IDS) enable enterprises to react to any security issues more quickly and efficiently by analysing network traffic and detecting malicious behaviour in real-time via the use of sophisticated algorithms and effective data processing methods [15]. As a result, attackers have a much smaller window of opportunity, and the possible consequences of security breaches are reduced.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

Challenges and Limitations of AI-based IDS

AI-based IDS have many benefits, but they also have drawbacks and restrictions [8]. False positives and false negatives are a major problem that may result in gaps in security coverage and an increased effort for security analysts [9]. Even though AI-based intrusion detection systems are meant to increase detection accuracy, in order to reduce these mistakes, it is crucial to constantly enhance the algorithms and system settings.

AI-based IDS's computational complexity might provide difficulties as well, especially for companies with little funding [10]. Large amounts of memory and processing power are often needed for machine learning algorithms and other AI approaches, which may call for the installation of specialised infrastructure and hardware. Therefore, it is important to carefully assess the costs and resource implications of deploying AI-based IDS.

Lastly, as AI-based IDS often analyse substantial amounts of private network data, utilising these systems presents data privacy issues [11]. Organisations must carefully assess the possible hazards involved with deploying AI-based IDS, including data storage, transport, and processing procedures, in order to ensure the privacy and security of this data. To reduce these risks, adherence to relevant data protection laws and the deployment of suitable security measures are crucial.

II. LITERATURE REVIEW

MIT is also developing machine learning defence strategies against cyberattacks. They describe a novel approach in their study "AI2: Training a big data machine to defend." There are four parts to their system. A supervised learning module, an outlier detection engine, a massive data processing system, and a way to get security analyst input. Their solution attempts to combine machine learning's speed and capacity for novel threat detection with the knowledge of security specialists. They use unsupervised machine learning, to be more precise. They selected unsupervised machine learning since assaults are always evolving and labelled data is not readily available. They create their labels inside the system, then utilise these labels to feed a supervised learning algorithm. A large data processing system is one that can take raw data and use it to extract characteristics from various entities [7]. One system that makes advantage of unsupervised learning is the outlier identification engine. It makes advantage of the large data processing system's characteristics. They use replicator neural networks, density, and matrix decomposition as their three techniques. After processing, the unsupervised system's output is presented to a security analyst. The result may be confirmed or denied by the security analyst. An algorithm for supervised learning receives the feedback. By using this feedback, the supervised learning algorithm builds a model that improves its ability to predict whether a new event is normal or abnormal. The system becomes more accurate as more input is received.

Role of ChatGPT and Similar AI Models in Enhancing IDS

AI-based anomaly detection looks for odd patterns in network traffic data by using machine learning methods like unsupervised or semi-supervised learning. Similar data points may be grouped together using unsupervised learning methods like clustering, which enables the AI model to discriminate between normal and pathological behaviour. On the other hand, semi-supervised learning algorithms increase their anomaly detection performance by combining labelled (known) and unlabeled (unknown) data.

In the context of intrusion detection systems, pattern recognition entails examining network traffic data to find signatures or patterns suggestive of malicious activity. AI models are very good at finding patterns in complicated and big datasets, particularly deep learning models like Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN). Historical data encompassing a variety of cyberattack and infiltration attempt types may be used to train these models [16]. The AI can identify comparable patterns in real-time network traffic data as it learns the hallmarks of known attack vectors, warning security personnel of possible dangers. Additionally, AI models are able to uncover new, unknown attack vectors that are similar to recognised dangers by generalising patterns acquired from past data.

These AI models may have the most effect when they use sophisticated data analysis and correlation approaches to decrease false positives. Furthermore, by leveraging security analysts' comments to retrain and fine-tune AI models over time, their capacity to recognise real threats is continuously improved, significantly lowering the amount of false positives [17].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

Case Studies with Verifiable Data across this investigation, we looked at effective AI-powered intrusion detection system (IDS) implementations across a variety of industries, with a focus on how artificial intelligence techniques like machine learning and neural networks may improve cyberattack detection and deterrence.

Banking and Financial Services

The banking and financial services industry is home to one outstanding example of effective AI-driven IDS implementation. In a research [18], Kanimozhi and Dr. T. Prem Jacob proposed an Artificial Neural Network-based solution for detecting botnet assaults, which pose a serious threat to these industries. The Canadian Institute for Cybersecurity provided the CSE-CIC-IDS2018 dataset, which was used to train the system. Amazon Web Services (AWS) was used for implementation. The results revealed a minimum false positive rate of 0.03%, an average ROC curve area of 0.999, and an unparalleled accuracy rate of 99.97%. The system's performance highlights the ability of AI-driven intrusion detection systems to monitor network traffic and identify cyber threats instantly.

AI-Enhanced Honeypots

DeepDig is an AI-integrated honeypot system developed by scientists at the University of Texas in Dallas that turns real network resources into lures by learning previous attacks [19]. This technique overcomes the limits of static deception technologies, which are susceptible to AI-capable adversaries since they do not learn from past assaults. By using machine learning techniques, DeepDig enhances the system's resistance to changing threats and increases its capacity to react to attackers' activities. Since actual assets are included into the honeypot, even the most proficient adversaries are unable to evade interaction with the trap, which allows the IDS to gradually learn and fortify its defences.

Deep Learning in Network IntrusionDetection

The use of deep learning algorithms for supervised network intrusion detection and unsupervised network anomaly detection was investigated in Xu et al.'s case study, cspecc.utsa.edu [20]. The study carefully evaluated deep learning's efficacy in network intrusion detection, demonstrating the promise of AI-powered methods in real-time analysis and detection of harmful data. This study contributes to the growing body of information about AI-driven intrusion detection systems and promotes the development of more sophisticated cybersecurity defence systems.

Future Directions

A ChatGPT-based intrusion detection system was put into place by following the first steps outlined in this article. The GPT-4 API from OpenAI was used for this [21]. There will be an explanation of the restrictions, theory, and proposed design.

ChatGPT IDS Design

It was chosen to utilise GPT-4 as the paradigm for creating an AI IDS. This is because of its extensive topic knowledge, precise problem-solving abilities, and capacity to carry out challenging orders. It is possible to employ an IDS, or current network traffic capture tool; in this study scenario, tcpdump was used. A low-profile command-line packet analyser called tcpdump has the ability to export network data in both CSV and pcap files [22]. The next stage is to analyse network traffic by either running GPT-4 separately or integrating it with the current network traffic capture tool. The incoming packet data would next be analysed by GPT-4, which would check it for malicious activities. This language model can scrape webpages to find current threats and payloads to compare with incoming network traffic since it is linked to the internet. As a result, the AI intrusion detection programme has the ability to identify more recent threats, which need ongoing patching in order for it to function. Figure 1 depicts the data flow and analysis.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

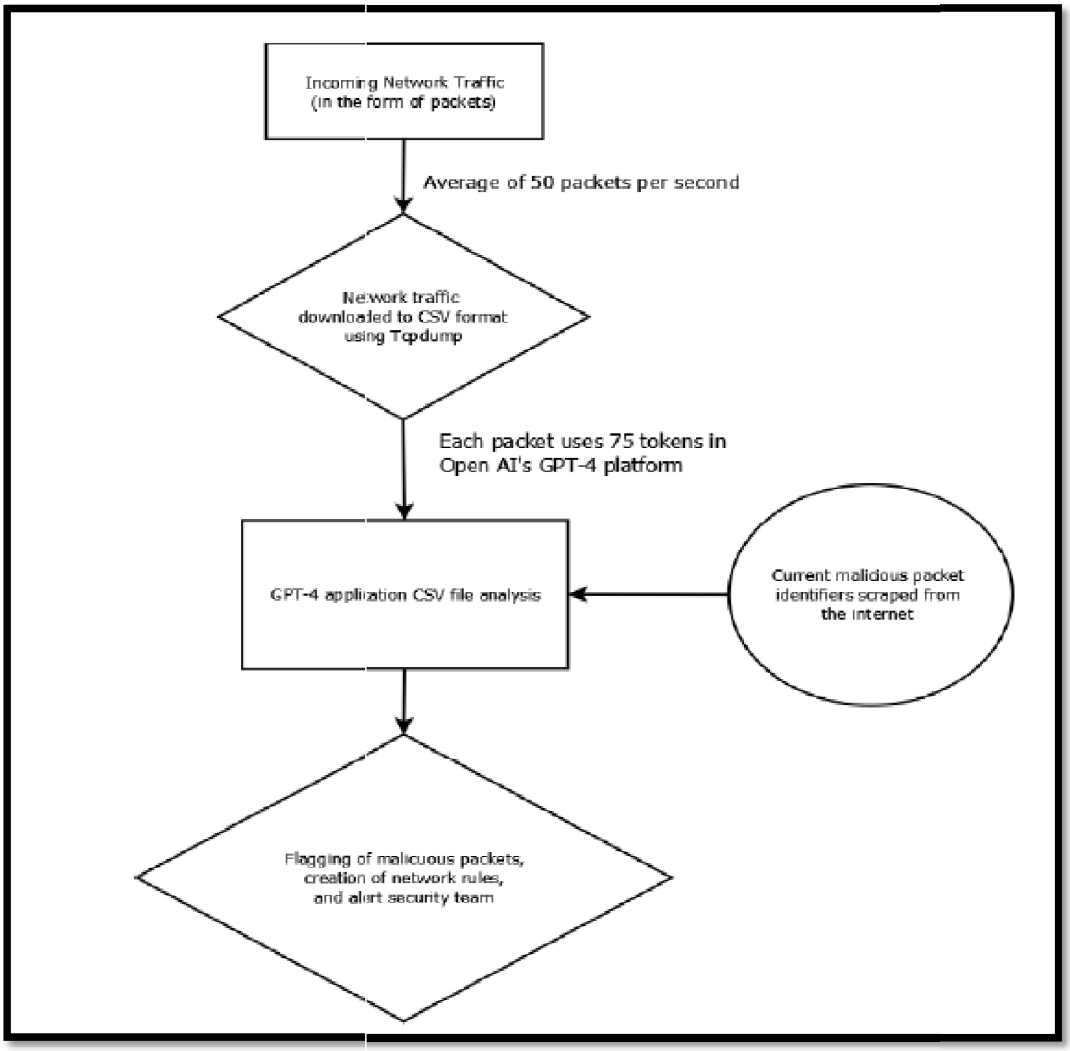

Figure 1: Data flow of proposed GPT-4 based IDSSource: Michal Markevych

Design Limitations

A little model that sampled less than 50 packets of data was used to create the architecture seen in Figure 1. A large-language model must be employed to transform the data from the packets into a vector database so that more packets may be analysed. Data is stored in vector databases and exported for analysis by tools like AI models. This limited the design's creation since the cost of vector databases increases with the volume of data examined.

The cost of the GPT-4 API, which is.03 cents for 1000 tokens, presented another difficulty. Let's take an example where a typical network receives 50 packets per second and has to analyse each one using 75 tokens (found using the data to token calculator). The cost of implementing this architecture is $6.75 for every minute the IDS system runs. Access to OpenAI's GPT-4 API waitlist, which gives users additional access to GPT-4 queries, might help to lessen this restriction.

III. CONCLUSION

ChatGPT and related AI models have enormous potential to greatly improve IDS. These improved systems provide more flexibility, improved pattern recognition, and accurate real-time detection and response capabilities by integrating AI algorithms. As a result, IDS is able to maintain an advantage over the ever-changing threat environment and provide

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

a stronger, more proactive defence against online attacks. Nevertheless, despite these advantages, there are still problems and topics that need further investigation. Improving AI-powered intrusion detection systems' accuracy and reducing false positives continue to be major priorities.

IDS is expected to become more effective and efficient as AI and machine learning continue to progress, which will reinforce its capacity to protect networks and computer systems from a wide range of cyberthreats. This is a methodology to do this work. Modern cybersecurity solutions are needed to defend critical infrastructure from emerging threats [23].

REFERENCES

[1]. Delamore B., Ko R.K.L. Chapter 9 - Security as a service (SecaaS)—An overview [Internet]. Ko R, Choo KKR, editors. ScienceDirect. Boston: Syngress; 2015 [cited2023 May 15].p 187–203. Available from:https://www.sciencedirect.com/science/article/abs/pii/B9780128015957000094

[2]. Niksefat S., Kaghazgaran P., Sadeghiyan B. Privacy issues in intrusion detection systems: Ataxonomy, survey and future directions. Computer Science Review. 2017 Aug;25:69–78.

[3]. Aljanabi M., Ismail M.A., Ali A.H. Intrusion Detection Systems, Issues, Challenges, andNeeds. International Journal of Computational Intelligence Systems. 2021;

[4]. Aljanabi M., Ismail M.A., Ali A.H. Intrusion Detection Systems, Issues, Challenges, andNeeds. International Journal of Computational Intelligence Systems. 2021;

[5]. Liao H.J., Richard Lin C.H., Lin Y.C., Tung K.Y. Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications [Internet]. 2013 Jan;36(1):16–24. Available from:https://www.sciencedirect.com/science/article/pii/S1084804512001944

[6]. Cybersecurity Spotlight – Signature-Based vs Anomaly-Based Detection [Internet]. CIS. Available from: https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight- signature-based-vs-anomaly-based-detection

[7]. Repalle S, Ratnam Kolluru V. Intrusion Detection System using AI and Machine Learning Algorithm. International Research Journal of Engineering and Technology.

[8]. Li W., Yi P., Wu Y., Pan L., Li J. A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network. Journal of Electrical and Computer Engineering [Internet]. 2014 [cited 2019 Nov 24];2014:1–8. Available from: https://www.hindawi.com/journals/jece/2014/240217/

[9]. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. 2010 IEEE Symposium on Security and Privacy [Internet]. 2010 [cited 2019 Dec 6]; Available from: https://ieeexplore.ieee.org/abstract/document/5504793/

[10]. Nobakht M., Sivaraman V., Boreli R. A Host-Based Intrusion Detection and Mitigation Framework for Smart Home IoT Using OpenFlow. 2016 11th International Conference on Availability, Reliability and Security (ARES). 2016 Aug;

[11]. Jagadish H.V., Gehrke J., Labrinidis A., Papakonstantinou Y., Patel J.M., RamakrishnanR., et al. Big data and its technical challenges. Communications of the ACM. 2014 Jul 1;57(7):86–94.

[12]. Valdovinos I., Perez-Diaz J., Choo K.K., Botero J. Emerging DDoS attack detection and mitigation strategies in software-defined networks: Taxonomy, challenges and future directions. Journal of Network and Computer Applications [Internet]. 2021 Aug 1 [cited2021 Sep 23];187:103093. Available from: https://www.sciencedirect.com/science/article/pii/S1084804521001156

[13]. Drewek-Ossowicka A., Pietrołaj M., Rumiński J. A survey of neural networks usage for intrusion detection systems. Journal of Ambient Intelligence and Humanized Computing. 2020 May 12;12(1):497–514.

[14]. Laghrissi F., Douzi S., Douzi K., Hssina B. IDS-attention: an efficient algorithm for intrusion detection systems using attention mechanism. Journal of Big Data. 2021 Nov 29;8(1).

[15]. Khraisat A., Gondal I., Vamplew P., Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity [Internet]. 2019 Jul 17;2(1). Available from: https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0038-7

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

[16]. Otoum Y., Nayak A. AS-IDS: Anomaly and Signature Based IDS for the Internet of Things. Journal of Network and Systems Management. 2021 Mar 4;29(3).

[17]. Kim A., Park M., Lee D.H. AI-IDS: Application of Deep Learning to Real-Time Web Intrusion Detection. IEEE Access. 2020;8:70245–61.

[18]. Kanimozhi V., Jacob T.P. Artificial Intelligence based Network Intrusion Detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC- IDS2018 using cloud computing. ICT Express. 2019 Apr;

[19]. William D. How AI can help improve intrusion detection systems [Internet]. GCN. Available from: https://gcn.com/cybersecurity/2020/04/how-ai-can-help-improve-intrusion-detection-systems/291266/

[20]. Fernández G., Xu S. A Case Study on Using Deep Learning for Network IntrusionDetection [Internet]. [cited 2023 May 15]. Available from:https://cspecc.utsa.edu/publications/files/Xu_2019_Case_Study_Deep_Learning_Net_I ntr_Detect.pdf

[21]. OpenAI. OpenAI [Internet]. OpenAI. 2019. Available from: https://openai.com/

[22]. tcpdump. TCPDUMP/LIBPCAP public repository. Tcpdumporg [Internet]. 2017; Available from: https://www.tcpdump.org

[23]. Dawson M., Bacius R., Gouveia L.B., & Vassilakos A. (2021). Understanding the challenge of cybersecurity in critical infrastructure sectors. Land Forces Academy Review, 26(1), 69-75.