HYBRIDMODELFOR DETECTING CYBERSECURITY THREATS BASED ON DEEP LEARNING WITH AN OPTIMISATION ALGORITHM

Manuscript Info

……..

Manuscript History
Received: xxxxxxxxxxxxxxx
Final Accepted: xxxxxxxxxxx
Published: xxxxxxxxxxxxxxx

Key words:-
cyberattack, threat, detection, neural network, optimisation, deep learning.

Abstract

……

Digital transformation and the Fourth Industrial Revolution have inevitably led to the emergence of new cybersecurity threats. Protection against these attacks is critical for individuals, businesses, organisations and countries as a whole. Effective threat detection depends on identifying both known and unknown risks and vulnerabilities as early as possible through a combination of visibility, analytics, and contextual awareness. Traditional risk assessment methods, in particular deterministic approaches to threat analysis, often fail to take into account the high level of uncertainty and variability in operating conditions. This article proposes an intelligent hybrid system for detecting cybersecurity threats based on a deep neo-fuzzy neural network with a combined optimisation algorithm for detecting and preventing relevant attacks.

……..

Introduction:-

Analysis of the security situation in the field of information and communication technologies, which is carried out on an ongoing basis by well-known global companies, shows that the global landscape of cyber threats is constantly changing [1,2,3]. For example, the annual report of the European Union Agency for Cybersecurity (ENISA) Threat Landscape 2024 identifies ransomware as one of the main threats, while phishing is noted as the most common initial vector for such attacks. Other significant threats include attacks on availability [4]. In addition, experts note that a wider range of attack vectors are currently emerging, such as zero-day exploits, disinformation and deep fakes, implemented using artificial intelligence (AI) tools. This has led to the emergence of even more malicious and widespread attacks that have a more destructive impact — advanced persistent threats (APTs) [5].

The huge amounts of data circulating in the digital environment today, on the one hand, and the danger of their leakage, on the other, make cybersecurity a high priority for individuals, industries, economic sectors, and the government of any country. According to analytical reports, cybercrime has become one of the world's largest shadow economies, with the total damage from cybercrime estimated at $10 trillion. More detailed information is presented in Table 1.

Table 1 Key indicators of global cyber threats (2020–2025) [6]

Indicator	2020	2021	2022	2023	2024	2025 (forecast)
Total damage from cybercrime (trillion dollars)	6,0	6,9	8,1	9.2	~9,5	~10,5
Number of data breaches (globally, thousands)	3,9	4,1	4,2	5,2	~6.0	~6,5
Number of DDoS attacks (millions)	9,8	11,2	13,1	15,4	~17.0	~18,5

Average cost of a data breach (millions of dollars)	3,86	4,24	4,35	4,45	~4,50	~4,60

In light of the above, it is clear that ensuring the security of information systems is essential, as the consequences of inadequate protection are manifold – theft, destruction or dissemination of confidential information (trade secrets), discrediting of personal data, substitution of information, blocking of access, restriction of functionality or complete shutdown of a computer network [7].

Traditional methods of detecting cyber threats are based on the use of statistical analysis of the security status at nodes using devices such as firewalls, intrusion detection and prevention systems, and antivirus software. However, such methods are insufficient for APTs, which highlights the need to use more advanced techniques based on AI tools such as intelligent data analysis, machine learning, neural networks, fuzzy logic, genetic algorithms, support vector machines, decision trees, and others.

The above-mentioned advanced methods allow for more accurate and higher-quality results, so a detailed analysis of their applicability in cybersecurity systems is a relevant area of scientific research, which determined the choice of topic for this article.

Literature review:

Today, there is a wide range of works in the scientific and expert community related to the detection of intrusions and attacks on information systems. Some of them concern the general classification of packets into normal or attacking categories, while others describe the features of detecting specific categories of attacks, such as RemotetoLocalUser and UsertoRoot attacks. This issue has been addressed in publications by Abdullah Al Mamun[8], Najah Kalifah Almazmomi [9], Kumari and Lee [10], Jiqiang Zhai *et al.* [11].

The possibility of using deep learning algorithms to check the entire information network infrastructure for viruses and illegally downloaded software is discussed by Iqbal H. Sarker [12], Ahmed Hawana*et al.* [13], E. A. Ichetovkin [14], Chaitanya Gupta et al. [15], Jiaqi Ruan, Gaoqi Liang [16].

A hybrid K-means approach using singular value principal component, which relies on methods such as improved information gain of K-means clustering for attribute extraction, singular value and principal component for feature reduction, is being developed by Asma Ahmed A. Mohammed [17], Jafar Majidpour and Hiwa Hasanzadeh [18], Qasem Abu Al-Haija and Ayat Droos [19], Tanzila Saba and Amjad Khan [20].

However, despite the wide range of publications, some problematic issues require clarification and further analysis. For example, methods for improving the self-learning ability of neural networks when analysing topological features need to be refined, which will ensure a high degree of generalisation and stable performance indicators. In addition, reinforcement learning applications for assessing cybersecurity threats require further development.

Thus, the purpose of this article is to examine the features of using deep learning with an optimisation algorithm to detect cybersecurity threats.

Research Methodology:

The research methodology is based on the application of system analysis, mathematical modelling and algorithmic optimisation methods, neural network and fuzzy modelling, as well as experimental verification of the hybrid architecture of a deep fuzzy neural network.

Results and discussion:

Deep learning is based on a multi-level representation of input data and can autonomously determine features

using a specific representation-based learning process. The ability of deep neural systems to analyse vast amounts of data and identify hidden patterns makes it an integral component of modern cybersecurity systems [21, 22, 23].

So, the task of detecting cybersecurity threats is as follows.

Let $D = \{(x_i, y_i)\}_{i=1}^{N}$ — be a sample of *N* examples, where x_i is the input vector, and y_i — is the output (in the case of classification — a vector of class probabilities, in the case of regression — a scalar variable). Let us denote the network parameters by *w*, and the posterior distribution can be written as $p(w|D)$. According to Bayes' formula:

$$p(w|D) = \frac{p(D|w)p(w)}{p(D)}$$

where $p(w)$ — is the prior distribution of parameters, $p(D|w)$ — is the likelihood of the data, and $p(D)$ — is the normalising constant, which is calculated by integrating over all possible values *w*.

Since accurate calculation $p(D)$ is quite a complex task, we suggest using a variational approximation: for this purpose, a family of distributions $p(w|\theta)$, parameterised by θ, introduced, and the Kulback-Leibler divergence between $p(w|\theta)$ и $p(w|D)$:

$$\theta^* = arg\min_{\theta} KL(q(w|\theta)||p(w|D))$$

The proposed cyber threat detection system is based on a hybrid model that uses deep learning mechanisms and an optimisation algorithm. Figure 1 shows the architecture of the threat detection system, implemented as a multi-stage data processing pipeline. This process includes sequential stages of feature space reduction, extraction of informative features, and their subsequent classification.

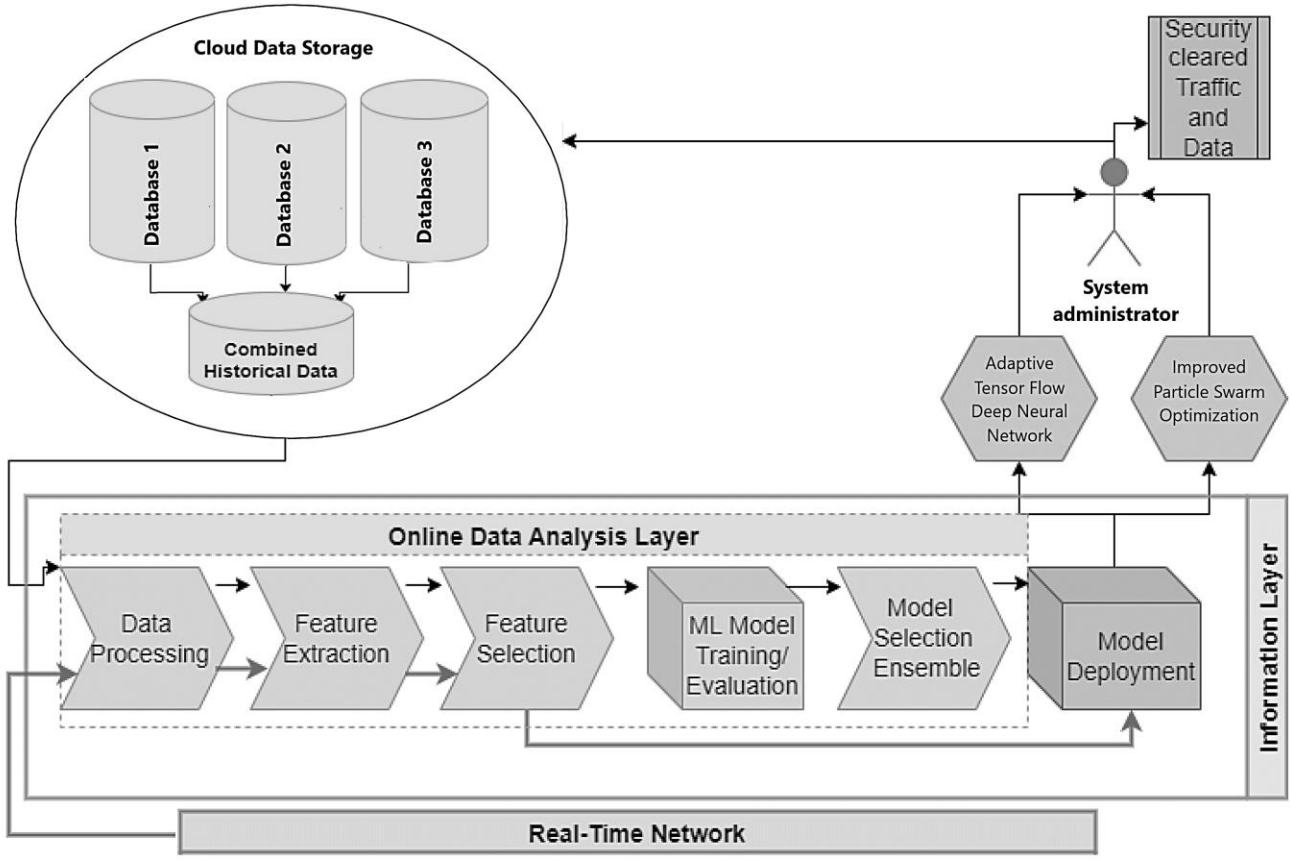

Fig. 1 Block diagram of cybersecurity threat detection based on deep learning with an optimisation algorithm (compiled by the author)

As shown in Figure 1, three databases are proposed for managing malicious and pirated software files in cloud storage. Raw network traffic data is stored in database 1, while historical data on malicious software is stored in database 2. The third database also accumulates the latest signatures of newly detected malicious attacks. The combined information storage module receives raw data from each database. The raw data undergoes preliminary processing, and important details are recorded in a log. The pre-processed data is then sent to the detection module, which analyses it for malware and other threats. This module is trained on signatures from databases 2 and 3. The proposed system alerts the administrator to take appropriate action if any malicious behaviour is detected on the network.

The proposed architecture is based on a deep neo-fuzzy neural network. It has a traditional multi-layer feedforward architecture, generally including s layers of information processing [24]. The input (zero) layer receives $x(k) \in R^n$ a vector of input signals:

$$x(k) = (x_1(k), x_2(k), \dots, x_n(k))$$

where k=1, 2, …, N – is the observation number in the training sample or the index of the current discrete time. The output signal of the network is a vector:

$$\hat{y}(k) = \left(\hat{y}_1(k), \hat{y}_2(k), \dots, \hat{y}_m(k)\right)^T \in R^m$$

Furthermore, to simplify the notation, we will also use the form:

$$x(k) \equiv o^{[0]}(k) = \left(o_1^{[0]}(k), \dots, o_{i_0}^{[0]}(k), \dots, o_{n_0}^{[0]}(k)\right)^T$$

$$\hat{y}(k) \equiv o^{[s]}(k) = \left(o_1^{[s]}(k), \dots, o_{i_s}^{[s]}(k), \dots, o_{n_s}^{[s]}(k)\right)^T$$

Thus, the input signal of the *p*-th layer (*p*=1, 2…, *s*) is a vector:

$$o^{[p-1]}(k) \equiv \left(o_1^{[p-1]}(k), \dots, o_{i_{p-1}}^{[p-1]}(k), \dots, o_{n_{p-1}}^{[p-1]}(k)\right)^T \in R^{n_{p-1}}$$

and the output is a vector:

$$o^{[p]}(k) = \left(o_1^{[p-1]}(k), \dots, o_{i_p}^{[p]}(k), \dots, o_{n_p}^{[p]}(k)\right)^T \in R^{n_p}$$

At the same time, the neo-fuzzy neural network contains $\sum_{p=1}^{s} n_p$ neurons. The node of this architecture is a neo-fuzzy neuron with n_{p-1} inputs and one output $o_{i_p}^{[p]}$.

Each i_p - th ($i_p = 1,2, \dots, n_p$) neo-fuzzy neuron of the *p*-th (p = 1,2, …, *s*) layer of the neo-fuzzy neural network contains n_{p-1} non-linear synapses $NS_{i_p i_{p-1}}^{[p]}$, each of which includes *h* membership functions $\mu_{i_p i_{p-1} l}^{[p]}$ ($l = 1,2, \dots, h$) and the same number of synaptic weight coefficients $w_{i_p i_{p-1} l}^{[p]}$, which are tuned during the learning process. Thus, this architecture has $\sum_{p=1}^{s} n_p n_{p-1}$ nonlinear synapses and $h \sum_{p=1}^{s} n_p n_{p-1}$ membership functions $\mu_{i_p i_{p-1} l}^{[p]}(o_{i_{p-1}}^{[p-1]})$ and the same number of tuned synaptic weight coefficients $w_{i_p i_{p-1} l}^{[p]}$.

The output signal of each nonlinear synapse $NS_{i_p i_{p-1}}^{[p]}$ can be recorded as:

$$f_{i_p i_{p-1} l}^{[p]}\left(o_{i_{p-1}}^{[p-1]}\right) = \sum_{l=1}^{h} w_{i_p i_{p-1} l}^{[p]}\, \mu_{i_p i_{p-1} l}^{[p]}(o_{i_{p-1}}^{[p-1]})$$

and the output signal of the neo-fuzzy neuron:

$$o_{i_p}^{[p]} = \sum_{i_{p-1}=1}^{n_{p-1}} f_{i_p i_{p-1} l}^{[p]}\left(o_{i_{p-1}}^{[p-1]}\right) = \sum_{i_{p-1}=1}^{n_{p-1}} \sum_{l=1}^{h} w_{i_p i_{p-1} l}^{[p]}\, \mu_{i_p i_{p-1} l}^{[p]}(o_{i_{p-1}}^{[p-1]})$$

As a membership function for nonlinear signals $NS_{i_p i_{p-1}}^{[p]}$ we suggest using the traditional triangular function, which satisfies the requirements of Ruspini's unit partition:

$$\mu_{i_p i_{p-1} l}^{[p]}\left(o_{i_{p-1}}^{[p-1]}\right) = \begin{cases} \dfrac{o_{i_{p-1}}^{[p-1]} - \mathrm{c}_{i_p i_{p-1} l-1}^{[p]}}{\mathrm{c}_{i_p i_{p-1} l}^{[p]} - \mathrm{c}_{i_p i_{p-1} l-1}^{[p]}}, & iff\ o_{i_{p-1}}^{[p-1]} \in [\mathrm{c}_{i_p i_{p-1} l-1}^{[p]}, \mathrm{c}_{i_p i_{p-1} l}^{[p]}) \\ \dfrac{\mathrm{c}_{i_p i_{p-1} l+1}^{[p]} - o_{i_{p-1}}^{[p-1]}}{\mathrm{c}_{i_p i_{p-1} l+1}^{[p]} - \mathrm{c}_{i_p i_{p-1} l}^{[p]}}, & iff\ o_{i_{p-1}}^{[p-1]} \in [\mathrm{c}_{i_p i_{p-1} l}^{[p]}, \mathrm{c}_{i_p i_{p-1} l+1}^{[p]}) \\ 0, & otherwise \end{cases}$$

Next, it is necessary to select a model optimisation algorithm that can improve the functionality of the deep neural network, thereby increasing the accuracy of detecting complex threats.

Within the scope of the task at hand, we propose using a combined particle swarm and genetic algorithm. The particle swarm algorithm ensures high accuracy and quick acquisition of an acceptable solution [25]. At the same time, the genetic algorithm is better suited for solving discrete problems and has more sophisticated mechanisms for combating local minima (through mutations and successful crossovers) [26]. The combined algorithm allows us to combine the advantages of both algorithms and thus achieve a quick and accurate solution to the task at hand. It is based on the idea of sequentially performing one iteration of the search by each of the basic algorithms (particle swarm and genetic algorithm), comparing the results found, and adding the best of the solutions found to each algorithm.

Step 1. Both algorithms are run simultaneously in parallel mode to synthesise the structure of the same neural network.

Step 2. One iteration of each algorithm is performed.

Step 3. After each iteration, the results found by both methods are compared and the best solution is selected. Let$Y_{pso}^{(i)}$ – the best solution found by the particle swarm algorithm at the *i*-th iteration, and $W_{ga}^{(i)}$ – the best solution found by the genetic algorithm. If $I(Y_{pso}^{(i)}) < I(W_{ga}^{(i)})$, that is, the solution obtained using the particle swarm algorithm provides a lower value of the quality function *I*, then we proceed to step 4a. Otherwise, we proceed to step 4b.

Step 4a. The worst solution of the genetic algorithm $W_{ga\_worst}^{(i)}$ is replaced by the solution $Y_{pso}^{(i)} W_{ga\_worst}^{(i)} \coloneqq Y_{pso}^{(i)}$ and the transition to step 5 is performed.

Step 4b. The worst solution of the particle swarm algorithm $Y_{pso\_worst}^{(i)}$ is replaced by the solution $W_{ga}^{(i)}, Y_{pso\_worst}^{(i)} \coloneqq W_{ga}^{(i)}$ and the transition to step 5 is performed.

Step 5. If both algorithms continue to run (i.e., the termination criterion is not met for either of them), proceed to step 2. The described approach is repeated until one of the algorithms terminates. The best solution found by both methods at the moment of termination is accepted as the final solution.

The results of modelling using particle swarm, genetic and combined algorithms are shown in Fig. 2.

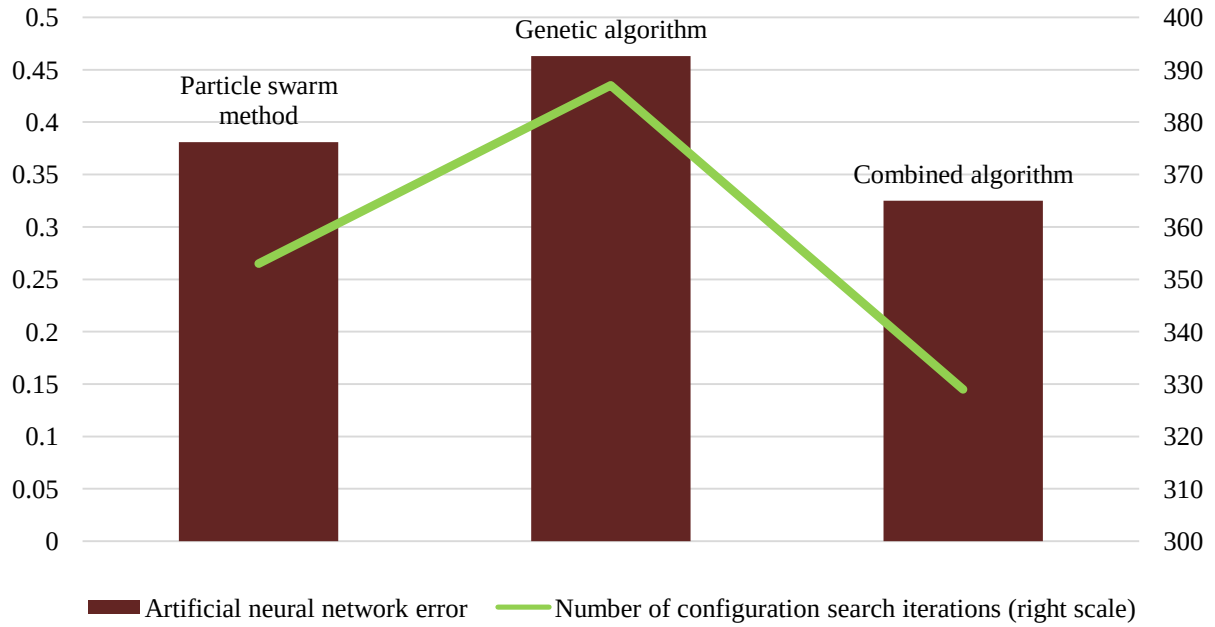

Fig. 2 Results of modelling the optimal structure of a neural network using various algorithms

As shown in Fig. 2, the combined algorithm allows for the lowest error and requires the fewest iterations to find the optimal neural network structure.

Conclusion:

Thus, summarising the results of the study, the following conclusions can be drawn:

Cybersecurity in the modern digital age is a critical area focused on protecting systems, networks, and information from malicious attacks. Organisations, businesses, governments, and countries are at great risk from cybercrime, which is becoming increasingly widespread, serious, complex, and diverse. The article describes an intelligent hybrid system for detecting cybersecurity threats based on a deep neo-fuzzy neural network with a combined optimisation algorithm for detecting and preventing such attacks.

References:

1. Danil Vilkhovsky (2024). AI capabilities in cybersecurity: detection, prevention and response to SQL injections, XSS, and CSRF attacks,Mathematical Structures and Modeling, Num 4 (72), pp. 111–124. DOI:10.24147/2222-8772.2024.4.111-124
2. Aulia Khanza, Firdaus Dwi Yulian, Novita Khairunnisa and Natasya Aprila Yusuf (2024). Evaluating the Effectiveness of Machine Learning in Cyber ThreatDetection. Journal of Computer Science and Technology Application 1(2):172-179. DOI:10.33050/ysdncf05
3. Mitchell Timken, Onat Gungor, Tajana Rosing and Baris Aksanli (2023). Analysis of Machine Learning Algorithms for Cyber Attack Detection in SCADA Power Systems, Conference: International Conference on Smart Communications and Networking (SmartNets), At: Istanbul, Turkey. DOI:10.1109/SmartNets58706.2023.10216147
4. Swapnil Chawande (2024). The role of Artificial Intelligence in cybersecurity, World Journal of Advanced

Engineering Technology and Sciences 11(2):683-696DOI:10.30574/wjaets.2024.11.2.0014
5. Yixian Liu and Yupeng Dai (2024). Deep Learning in Cybersecurity: A Hybrid BERT–LSTM Network for SQL Injection Attack Detection, IET Information Security. Volume 20, Issue 17. P. 25-29. DOI:10.1049/2024/5565950
6. Rasim Alguliyev and Ramiz Shikhaliyev (2024). Computer Networks Cybersecurity Monitoring Based on Deep Learning Model, Security and Privacy. 8(1), P. 114-116. DOI:10.1002/spy2.459
7. Dmitrii Bykov (2025). THE ROLE OF MACHINE LEARNING METHODS IN IDENTIFYING CYBER THREATS BASED ON TEXT DATA, Universum Technical sciences 4(133)**DOI:10.32743/UniTech.2025.133.4.19826**
8. A. Al Mamun, H. Al-Sahaf, I. Welch, and S. Camtepe, " Advanced Persistent ThreatDetection: A ParticleSwarmOptimizationApproach," in *2022 32nd International Telecommunication Networks and Applications Conference (ITNAC)* (IEEE, 2022), 1–8.
9. Najah Kalifah Almazmomi (2025). Advanced Persistent Threat Detection Using Optimized and Hybrid Deep Learning Approach, Security and Privacy. Vol. 8, Issue 2, P. 76-82.DOI:10.1002/spy2.70011
10. I. Kumari and M. Lee (2023). "A Prospective Approach to Detect Advanced Persistent Threats: Utilizing Hybrid Optimization Technique," *Heliyon* **9**, no. 11 (2023): e21377, **https://doi.org/10.1016/j.heliyon.2023.e21377**.
11. Jiqiang Zhai, Zhe Li, Hong Miao, Zekun Li, Xinyi Zhou, Hailu Yang (2025). Automatic Generation of Cybersecurity Teaching Cases Using Large Language Models, Computer Applications in Engineering Education, Volume 33, Issue 5, P. 203-211.DOI:10.1002/cae.70081
12. Iqbal H. Sarker (2023). Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview, Security and Privacy, 6 (2). DOI:10.1002/spy2.295
13. Ahmed Hawana, Emad Hassan, Walid El-Shafai and Sami A. El-Dolil (2025). Enhancing Malware Detection With Deep Learning Convolutional Neural Networks: Investigating the Impact of Image Size Variations, Security and Privacy, 8 (2), P. 91-99. DOI:10.1002/spy2.70000
14. E. A. Ichetovkin (2025). Investigating the resistance of intrusion detectionsystemswith machine learning components to adversarialattacks, *Vestnik of Astrakhan State TechnicalUniversity. Series: Management, Computer Sciences and Informatics, Number 2, Pages 76–87* **DOI: https://doi.org/10.24143/2072-9502-2025-2-76-87**
15. Chaitanya Gupta, Ishita Johri, Kathiravan Srinivasan and Yuh-Chung Hu (2022**).** A SystematicReview on Machine Learning and Deep Learning Models for Electronic Information Security in Mobile Networks, Sensors, 22(5):2017. DOI:10.3390/s22052017
16. Jiaqi Ruan and Gaoqi Liang (2023). Deep learning for cybersecurity in smart grids: Review and perspectives, Energy Conversion and Economics, 4(4), P. 59-64. DOI:10.1049/enc2.12091
17. Asma Ahmed A. Mohammed (2025). Improving Intrusion DetectionSystems by Using Deep Learning Methods on Time Series Data, Engineering, Technology and Applied Science Research 15(1):19267-19272 **DOI:10.48084/etasr.9417**
18. Jafar Majidpour and Hiwa Hasanzadeh (2020). Application of deep learning to enhance the accuracy of intrusion detection in modern computer networks. Bulletin of Electrical Engineering and Informatics

(BEEI),9(3)**DOI: https://doi.org/10.11591/eei.v9i3.1724**

19. Qasem Abu Al-Haija and Ayat Droos (2024). A comprehensive survey on deep learning-based intrusion detection systems in Internet of Things (IoT), Expert Systems, 42 (2), P. 71-77. DOI:10.1111/exsy.13726
20. Tanzila Saba, Amjad Rehman Khan, Tariq Sadad and Seng-phil Hong (2022). Securing the IoT System of Smart City against Cyber Threats Using Deep Learning, Discrete Dynamics in Nature and Society, (1):1-9DOI:10.1155/2022/1241122
21. Shilpa Ankalaki, A Aparna Rajesh, M Pallavi, Geetabai S Hukkeri, Tony Jan and Ganesh Naik (2025). Cyber Attack Prediction: From Traditional Machine Learning to Generative Artificial Intelligence, IEEE Access PP(99):1-1. DOI:10.1109/ACCESS.2025.3547433
22. HilalahAlturkistani and SuriayatiChuprat (2024). Artificial Intelligence and Large Language Models in Advancing Cyber Threat Intelligence: A Systematic Literature Review. Research Square (Research Square). DOI:10.21203/rs.3.rs-5423193/v1
23. Sharmin Aktar, Abdullah Yasin Nur (2023). Towards DDoS attack detection using deep learning approach, Computers & Security, Vol 129, 103251. https://doi.org/10.1016/j.cose.2023.103251
24. Kumar Reddy Mallidi and Rajeswara Rao Ramisetty (2025). Optimizing Intrusion Detection for IoT: A Systematic Review of Machine Learning and Deep Learning Approaches With Feature Selection and Data Balancing, Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 15(2),P. 223-234. DOI:10.1002/widm.70008
25. Jeferson Arango-López, Gustavo Isaza, Fabian Ramirez, Nestor Duque, Jose Montes (2024). Cloud-based deep learning architecture for DDoS cyber attack prediction, Expert Systems, 42(1), P. 41-45. DOI:10.1111/exsy.13552
26. Pavel A. Vasilevskiy and Elena V. Bulgakova (2025). Exploring the Use of Machine Learning to IdentifyThreats in Powershell Scripts, Conference: 2025 Systems of SignalsGenerating and Processing in the Field of on Board Communications. DOI:10.1109/IEEECONF64229.2025.10948055

Corresponding Author: oboulhas@yahoo.fr

1. Address**:-**Ecole Nationale Supérieure Polytechnique, Université Marien NGOUABI, Republic of Congo