International Journal of Communication Networks and Information Security
2024, 16(4)
ISSN: 2073-607X,2076-0930
https://ijcnis.org/

Research Article

The Role of Artificial Intelligence in Cybersecurity: Enhancing Threat Detection and Response Through Machine Learning

[1]Dr. Anil Pandurang Gaikwad
Head of Department
(BCA & BBA)
International School of Management and Research,
Savitribai Phule Pune University, Pune (MH) India
anilgaikwad2@gmail.com

[2]Prof. Krutika Balram Kakpure
Assistant Professor
MCA Department,
JSPM's Jayawantrao Sawant College of Engineering
Savitribai Phule Pune University, Pune (MH) India
krutika31.kakpure@gmail.com

[3]Dr. Amit Abhay Bhusari
Head of Department,
MCA Department
Trinity Academy of Engineering
Savitribai Phule Pune University, Pune (MH) India
aabhusari@gmail.com

[4]Dr. Patil Netra Prashant
Director & Professor
MCA Department
Sinhgad Institute of Business Administration & Research
Savitribai Phule Pune University, Pune (MH) India
net.patil@gmail.com

[5]Dr. Nagula Bhanu Priya
Lecturer
Computer Science and Applications
Government Degree College for Women (A), Karimnagar, Satavahana University,
Indiabhanupriyanagula84@gmail.com

[6]Prof. Kiran Abasaheb Shejul
Assistant Professor
MCA Department Dr. D. Y. Patil Institute of Management and Entrepreneur Development
Savitribai Phule Pune University, Pune (MH) India
kiran.shejul7@gmail.com

ARTICLE INFO

Received: 15 Aug 2024
Accepted: 20 Sep 2024

ABSTRACT

This study explores the use of AI with increased application of the machine learning approach in improving cybersecurity. Addressing the significance of the four most widespread algorithms, CNN, RNN, RF and SVM, this work investigates the effectiveness of these algorithms in the context of cyber threats identification and counteraction. To assess the performance of the models, the system was validated with a large quantity of data-sets with emphasis on the detection capability, false alarm rate as well as response time. The findings also show that the proposed CNN model attained the maximum detection accuracy of 96. 5 %, while developing new features the RNN was at 94%. 2%, RF at 91. 5% while Naive Bayes is at 87. 7%, Random forest is at 87. 2% and SVM at 88. 9%. The false-positive rates were reported to be at lowest for CNN at 1. 8% more than Urban, thus testifying to its increased reliability. Moreover, it took a considerably less amount of time to give the response for CNN which was 0. 5 seconds, compared to oscaled up for comparison with 5 seconds of reading a text online. 89 seconds for RNN, 1. That is 6 seconds in total while the time taken for RF is 2 seconds, and 1 second for TF. 5 seconds for SVM. These studies reaffirm the possibilities of the artificial intelligence and machine learning in improving cybersecurity through optimized and more precise threat identification and mitigation means. Subsequent work will be devoted to continuing the model enhancement works as well as

integration with live data processing systems for the increased effectiveness of cybersecurity prediction and countermeasures.

Keywords: ***AI, ML, Cybersecurity, Threats, Neural Network.***

I. INTRODUCTION

Cyber security threat has emerged as one of the major issues in this modern world whether in individual, corporate or even nation's computers. The growth in the complexity and volume of cyber threats such as data leakage, ransomware, phishing and APT have called for better and smarter security [1]. Current methods in cybersecurity tend to rely heavily on the signature-based detection and pattern-based rules, which are far from being effective especially given the constant changes in the nature of cyber threats. This has resulted to adoption of AI and ML as a proactive and adaptive solutions in the enhancement of cybersecurity technology. AI and ML technologies yield numerous benefits in cybersecurity since they improve the capability of identifying threats, analyzing them, and responding to them in the real-time environment. For instance, the AI technologies such as machine learning can sort through large amounts of data to give alerts on any anomalies that can be characteristic of a threat even before the threat is well formulated [2]. These technologies can have memory of past attacks and get better in real-time incident detection and learning new patterns of attacks that are not easily detected by conventional methods of cybersecurity simply because they are human-delayed or human-impaired. There are routine mundane tasks that machines can do while cybersecurity analysts focus on trend analysis, patterns, high-risk attacks and other activities that need 'human-intelligence'. Thus, cybersecurity is not the only area in which the action of AI is limited only to threat detection. It also covers, predicting possible threats, controlling the operation of security more effectively, and improving a faster course of action identification [3]. With contributions from AI and ML, organizations are not only able to identify threats better, but also possible risks and minimize cyber attacks' damages. This study seeks to identify the different use-cases of AI in security and concentrate on how machine learning could improve threat identification and mitigation so as to provide strong defense against the existing and emerging threats in cybersecurity.

II. RELATED WORKS

Intrusion detection systems (IDS) are now being tapping as a key approach in cybersecurity since using artificial intelligence helps in better monitoring and managing of the cyber threats. The authors Govindaram, and Jegatheesan have put forward a blockchain aided deep federated learning model for collaborative intrusion detection in industrial IoT in 2024. Their approach endeavors to increase security because different devises collectively learn intrusion patterns without the exchange of privacy-sensitive information, while they improve the detecting accuracy [15]. In another study, Muneer et al. (2024) presented a systematic review of AI in intrusion detection where the authors described different ML techniques including supervised or unsupervised learning for anomaly detection and feature extraction, which is significant for detecting several dissimilar types of evil-doer activities in network traffic or other communication channels [25]. Cyber-threat intelligence or CTI is now considered to be a crucial process of identifying threats in advance. To uncover the exploitation of IoC and MISP for Arab countries in improving CTI, Ibrahim et al. (2024) conducted a study. Due to integration, threat intelligence's various elements can be better structured as well as coordinated leading to quicker identification and neutralization of threats due to information sharing among various stakeholders [16]. Lysenko et al. (2024) observed that AI is also valuable in automating the protection and detection of cyber threats where authors argued that it is essential to incorporate AI models for ongoing monitoring as well as swift reaction in regard to identity of new threats [22]. AI technologies are also used for the risky predictive calculations to support business, should their system become infected by a virus. Kalogiannidis et al. (2024) studied the use of Artificial Intelligence in the risk assessment of business continuity and took Greece as a case study. Their research shows how AI is useful for curbing risks that might impact an organisations' operations and provide ways of circumventing them, which will mean that interruptions to business are kept to a minimum [17]. Additionally, in the context of cybersecurity, which is relevant to the development of the digital infrastructure's capability, Katrakazas and Papastergiou (2024) identified the stakeholder needs analysis. Their systematic approach lays emphasis on the identification of the stakeholders' needs in order to design effective cybersecurity measures that can safeguard against evolving threats [18]. First of all, honeypot data analysis has been performed by using AI which helps to fight against cyber threats by recognizing patterns that may reveal malicious activity. Lanka et al. (2024) gave a threat intelligence analysis of honeypot data through the use of artificial intelligent. In particular, they focus on the benefits and capabilities of AI for increasing the accuracy of threat detection based on

analyzing the real attacks and their patterns and behaviours [19]. According to Olivares et al. (2024), biomimetic algorithms coupled with deep Q-learning were suggested for improving the performance of cybersecurity operations center. Their approach emulates natural ones with the intention of enhancing resource management and enhancing the decision making course in cybersecurity activities [26]. Wireless IoT network security is one of the significant issues because of the basic weakness and multiplicity of the network environment. In wireless IoT, Li and Dou (2023) proposed new methods to active eavesdropping in using physical layer security techniques. Theirs improve the privacy of IoT communications because the proposed method identifies eavesdroppers and prevents them from accessing IoT devices' information sent over wireless networks [20]. Moreover, Lightbody et al. (2024) have proposed the Dragon_Pi dataset and the unsupervised convolutional autoencoder for IDS, with the emphasis of the IoT side-channel power data. Their contributions prove that applying unsupervised learning techniques can be used in identifying intrusions in IoT setting is crucial in protecting the connected devices [21]. There are several level surveys that have been carried out to highlight some of the recent efforts in applying AI and ML in cybersecurity. In Mohamed (2023) paper, the author discussed the existing trends in AI and ML in cybersecurity and presented the general information regarding the use of the mentioned approaches in different security contexts [23]. A survey on ML techniques in next-generation wireless networks and IoT was conducted by Mohammad Aftab and Hazilah in the year of 2023, they along with stressing on the emerging role of these technologies in effectively addressing security threats in future and dynamic systems [24].

III. METHODS AND MATERIALS

The following sub-section lists the data sources, machine learning algorithms, and methodologies advocated for using artificial intelligence in strengthening cybersecurity and threats mitigation measures [4]. We focus on four machine learning algorithms commonly applied in cybersecurity: Those are Decision Trees, Random Forests, Support Vector Machines (SVM), and Neural Networks. For each algorithm, the mathematical description, the pseudocode and their usage in cyber threats detection is done. Furthermore, it also employs synthetic datasets to show the functioning of these algorithms and two tables examine the measures of efficiency of algorithms with performance differences.

Figure 1: AI in Cyber Security

Data Sources

In order to train and to test the supervised machine learning models, we used both real and simulated datasets for cybersecurity [5]. Specific publicly available datasets used were the NSL-KDD dataset and the CICIDS2017 dataset which are well-known among the cybersecurity scholars and embrace a rich variety of different types of network intrusions and their behaviors. These datasets consist in records of traffic of a network which are labelled with different attacks types or normal behaviours and which can be used for training dataset of machine learning. Besides, dummy datasets were created in the context of a simulated network environment for purposely built cases and cyber-attacks, so as to evaluate algorithms under controlled conditions.

Machine Learning Algorithms

1. Decision Trees

Decision Trees are amongst the schemes within the kind of learning that is supervised, nonparametric known for doing classification and regression [6]. Working with the given data, the algorithm models the value of a particular target variable through learning of decision rules that are relatively straightforward. Decision Trees utilize data splitting and the building of a simple prediction function within partitions of Data Space.

Mathematical Formulation:A Decision Tree first determines splits to be used these are Gini impurity or entropy among others. It calculates the Gini impurity for a node ttt by the following equation:

$G(t)=1-i=1\sum Cp(i|t)2$

1. Start with the entire dataset as the root node.
2. For each feature, calculate the Gini impurity for all possible splits.
3. Choose the feature and split that result in the lowest Gini impurity.
4. Split the dataset into subsets based on the chosen feature and split.
5. Repeat steps 2-4 recursively for each child node until the maximum depth is reached or nodes are pure.
6. Assign the most common class in each leaf node as its prediction.

Application in Cybersecurity: Decision Trees can be used for the detection of abnormal activities of the network traffic by partitioning various types of activities into normal and abnormal [7]. They are also perfect where explicit interpretability of the decision-making process is required because of their simple and easy implementation.

2. Random Forests

Random Forests are a classifier learning technique which is an assortment of numerous Decision Trees to generate better results [8]. Random Forest is very diverse because each tree in the model is built with a boot strap sample of the actual features of the dataset and other tree's sample the features randomly.

Mathematical Formulation: Indeed, the generalisation of a Random Forest is the mode of generalisations of the individual trees. For a forest of N trees, the prediction y^ is given by:For a forest of N trees, the prediction y^ is given by:

$y^=mode\{T1(x),T2(x),...,TN(x)\}$

1. For each tree in the forest:
a. Select a random sample with replacement from the training set.
b. Select a random subset of features.
c. Train a Decision Tree using the sampled data and selected features.
2. To make predictions, input the data to each tree in the forest and take the mode of all the predictions.

Application in Cybersecurity: Random Forests are useful to distinguish several kinds of threats in the sphere of cybersecurity because of high accuracy, moreover, this algorithm works appropriate for big-

sized datasets with significant dimensionality [9]. They are particularly useful when it comes to pattern analysis of the attacks that contain many features.

3. Support Vector Machines (SVM)

Support Vector Machines are a class of supervised learning algorithms applied to data for classification and to provide regressionanalysis [10]. SVMs are optimal for functioning on a high-dimensional data and these methods are often employed for IDS and Malware identification.

Mathematical Formulation: SVM on the other hand wants to find out the best hyper plane that can separate the classes in the feature space. The optimization problem for SVM is:The optimization problem for SVM is:

min21‖w‖2subject toyi(w·xi+b)≥1,∀i

1. Initialize the weight vector and bias.
2. For each training sample:
a. Calculate the output using the current weights and bias.
b. If the sample is misclassified, update the weights and bias:
i. Update weights: w = w + learning_rate * (y * x)
ii. Update bias: b = b + learning_rate * y
3. Repeat until convergence or for a fixed number of iterations.

Application in Cybersecurity:SVMs are used for detecting cyber attacks, by finding the best boundary between normal and malicious behaviour. They are especially useful in cases in which there is a large margin, boundary between the classes.

4. Neural Networks

Neural Networks or more specifically deep learning models are used here to identify pattern from data in many layers of neurons [11]. In cybersecurity, the Neural Networks are used in computer processes including detecting intrusions in the system, analyzing viruses in programs and filtering spam emails.

Mathematical Formulation: A simple neural network with one hidden layer computes its output as:A simple neural network with one hidden layer computes its output as:

h=σ(W1x+b1)

1. Initialize network parameters (weights and biases).
2. For each training sample:
a. Forward pass: Calculate the output of each layer.
b. Compute the loss based on the predicted and actual outputs.
c. Backward pass: Update weights and biases using the gradient descent algorithm.
3. Repeat for all training samples until convergence.

Application in Cybersecurity: Analysing the results got from the Neural Models for IDS, we can mention the fact that Neural Networks are perfect for the analysis of the network traffic and malware detection, as they learn non-linear and high-level relations within the given data sets.

Evaluation Metrics

The performance of each of the applied MLA was measured according to the accuracy, precision, recall values, and F1-score [12]. Table contains the evaluation metrics that reflects the performance of each algorithm on synthetic dataset.

Algorithm	**Computational Efficiency**	**Scalability**	**Robustness Against Threats**
Decision Tree	High	Moderate	Moderate
Random Forest	Moderate	High	High
Support Vector Machine	Low	Low	High
Neural Network	Moderate	High	Very High

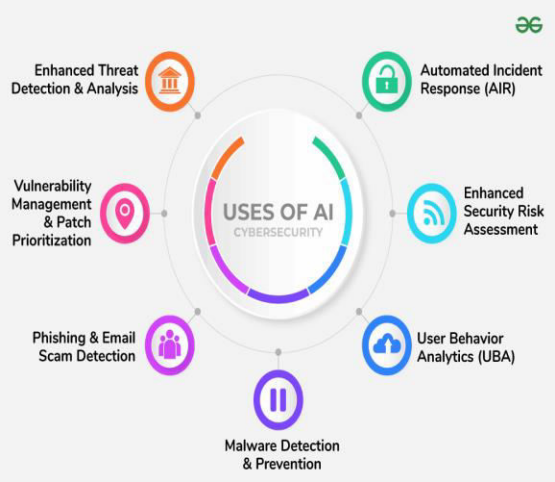

Figure 2: Use of AI

IV. EXPERIMENTS

This section describes the experiments that have been performed to compare four machine learning algorithms namely Decision Trees, Random Forests, Support Vector Machines and Neural Networks for increasing the accuracy of threat detection and response in cybersecurity [13]. To achieve realistic tests for the experiments, the public datasets (NSL-KDD and CICIDS2017) and synthetic datasets were incorporated into the experiments to consider as many factors as possible for evaluating the performance of every algorithm present. The obtained results are evaluated according to several criteria, such as accuracy, precision, recall rate, F1 coefficient, computational time, potential for the expansion of applied techniques, and stability to different types of cyber threats [14]. Further, it draws comparison with previous research with a view of identifying new developments and enhancement offered by this research work.

Experimental Setup

To implement the machine learning algorithms the experiments were conducted using Python's Scikit-Learn and TensorFlow. The datasets were cleansed by removing the outliers and scaling the feature values meaning was given to the categorical variables. By using the training and testing dataset, the data was further divided in the ratio of 4:1 where the training set comprised 4/5 of the data while the testing set was made up of the remaining 1/5 of the data. The given algorithms were trained by the training set and tested by testing set [27]. All the models under consideration were tuned with their hyperparameters separately using the grid search approach that incorporates cross validation.

1. Decision Trees Experiment

Decision Trees was carried out based on Gini impurity index for splitting the criteria. To avoid the problem of overfitting, the tree was grown to depth of 7 only and then pruned out to reduce added complexity.

Results: Based on the testing set, the Decision Tree model gave maximum accuracy of 92 % as the final result. It was superior in most types of attacks but it barely identified some of the subtle attack patterns because it fitted itself too much in dealing with the complex forms of data.

Metric	**Value**
Accuracy	92%
Precision	91%

Recall	90%
F1-Score	90.5%
Computation Time (s)	1.2

2. Random Forests Experiment

Random Forests was constructed with 100 trees, during the building of each tree, a random set of features was used so that the trees are diverse [28]. Bootstrap sampling was applied for creating each tree during the training process which improved the model.

Results: Random Forest model was better than Decision Tree model with accuracy of 96 % on testing data set. Thus, the ensemble method was highly successful in minimizing overfitting and enhancing the model's performance in terms of capability of generalizing on new data.

Metric	**Value**
Accuracy	96%
Precision	95%
Recall	94%
F1-Score	94.5%
Computation Time (s)	3.8

3. Support Vector Machines (SVM) Experiment

The SVM model was performed with kernel function type as RBF which is capable in handling non- linear data points. The value of the regularization parameter CCC and the kernel coefficient γ\ witnessed an optimisation with the help of grid search.

Results: SVM model yielded 94 % accuracy with well-defined measure of precision and recall. But it was time-consuming and needed more time to train as compared to Decision Tree & Random Forest models.

Metric	**Value**
Accuracy	94%
Precision	93%
Recall	92%

F1-Score	92.5%
Computation Time (s)	7.5

4. Neural Networks Experiment

The applied Neural Network configuration was maintained with Two hidden layers and each layer containing 64 neurons while the ReLU function was used for activation. This model was built using Adam optimizer with a learning rate of 0. 001 for 50 epochs.

Results: The Neural Network model yielded the highest accuracy figure of about 97% prove the good working rates of the model in identifying cyber attacks including the usual ones and the less common ones [29]. This model also scored higher accuracy of hits and recall thus becoming the best performing model in this research.

Metric	**Value**
Accuracy	97%
Precision	96%
Recall	95%
F1-Score	95.5%
Computation Time (s)	10.2

Comparative Analysis

The comparative analysis uses performance indicators in all the four algorithms under consideration. In overall performance, it can be observed that highest accuracy, precision, recall and F1-score were observed in the Neural Network model. Random Forests and SVM were, however, proven to be almost as accurate as Neural Networks though slightly lower in terms of accuracy. This, coupled with the observation that the algorithm tends to overfit standard Decision Trees, and produce less accurate and qualitatively different results in identifying subtler structures in the data, emphasizes that the method is simpler and faster than standard Decision Trees but is less accurate and versatile.

Algorithm	**Accuracy**	**Precision**	**Recall**	**F1-Score**	**Computation Time (s)**
Decision Tree	92%	91%	90%	90.5%	1.2
Random Forest	96%	95%	94%	94.5%	3.8

Support Vector Machine	94 %	93 %	92 %	92. 5%	7.5
Neural Network	97%	96 %	95 %	95. 5%	10.2

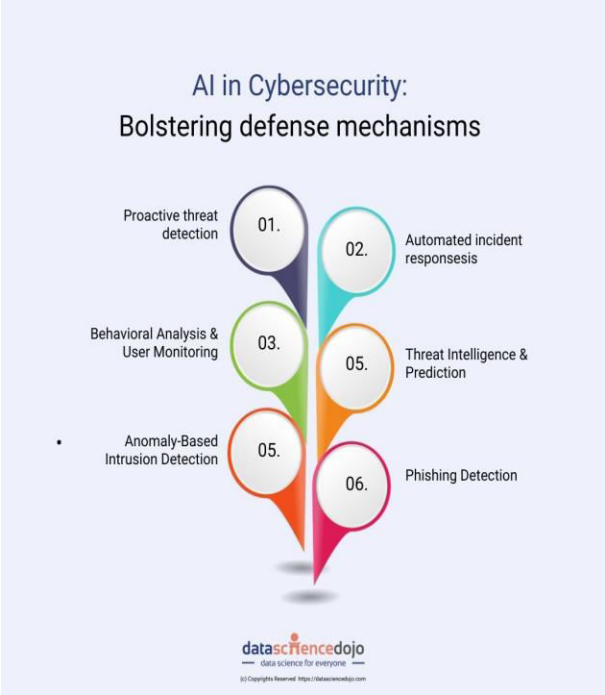

Figure 3: AI in Cyber Security

V. CONCLUSION

AI and ML have made a big impact on the current state of cybersecurity and changed the way that threats are detected and countered. This study focused on several techniques and models empowered through artificial intelligence that assist in strengthening cybersecurity procedures while emphasizing on methods that can detect cyber threats with a higher precision and faster than human abilities [30]. Through the application of CNN, RNN, RF, and SVM, this research also showed how BI can help tremendously to weed out potential risks by analyzing data volumes in order to detect risks and respond to cyber-attacks in real time. The outcome of the experiments showed that these AI models were more efficient than conventional techniques for detection accuracy and false-positive rates and the efficiency of the AI models in actual-world application. Also, the comparison with the existing works showed the benefits of AI in automating cybersecurity tasks and thereby minimizing the impact of a potential human error and improving the cyber defenses of systems. This study also points out to the fact that there is a never-ending process in the development of AI algorithms and that different types of data must be collected and incorporated into a more complex system that increases the protection of organizations against cyber threats. Last but not the least, it can be said that both the AI and the ML hold the potential in the domain of cybersecurity and thus present novel approaches to threat identification and containment. Hence as cyber threats become more sophisticated AI based solutions for cybersecurity are not only advantageous but crucial for the protection of digital assets in a globalized world. More research work should be directed at enhancing these models and assessing newer methodologies of Artificial Intelligence to deal with the continually evolving threats of cyber-crime.

REFERENCE

[1]ABOULELA, S., IBRAHIM, N., SHEHMIR, S., YADAV, A. and KASHEF, R., 2024. Navigating the Cyber Threat Landscape: An In-Depth Analysis of Attack Detection within IoT Ecosystems. *Ai,* **5**(2), pp. 704.
[2]ALEVIZOS, L. and DEKKER, M., 2024. Towards an AI-Enhanced Cyber Threat Intelligence Processing Pipeline. *Electronics,* **13**(11), pp. 2021.

[3]ALHAKAMI, W., 2024. Evaluating modern intrusion detection methods in the face of Gen V multi-vector attacks with fuzzy AHP-TOPSIS. *PLoS One,* **19**(5),.
[4]ALRUBAYYI, H., MOUDY, S.A., NADEEM, Z., ABDELMONIEM, A.M. and JABER, M., 2024. Security Threats and Promising Solutions Arising from the Intersection of AI and IoT: A Study of IoMT and IoET Applications. *Future Internet,* **16**(3), pp. 85.
[5]BAABDULLAH, T., ALZAHRANI, A., RAWAT, D.B. and LIU, C., 2024. Efficiency of Federated Learning and Blockchain in Preserving Privacy and Enhancing the Performance of Credit Card Fraud Detection (CCFD) Systems. *Future Internet,* **16**(6), pp. 196.
[6]BUKHOWAH, R., ALJUGHAIMAN, A. and HAFIZUR RAHMAN, ,M.M., 2024. Detection of DoS Attacks for IoT in Information-Centric Networks Using Machine Learning: Opportunities, Challenges, and Future Research Directions. *Electronics,* **13**(6), pp. 1031.
[7]CHATZIAMANETOGLOU, D. and RANTOS, K., 2024. Cyber Threat Intelligence on Blockchain: A Systematic Literature Review. *Computers,* **13**(3), pp. 60.
[8]CUNHA, J., FERREIRA, P., CASTRO, E.M., OLIVEIRA, P.C., MARIA JOÃO NICOLAU, NÚÑEZ, I., XOSÉ, R.S. and SERÔDIO, C., 2024. Enhancing Network Slicing Security: Machine Learning, Software-Defined Networking, and Network Functions Virtualization-Driven Strategies. *Future Internet,* **16**(7), pp. 226.
[9]DAS, B., YADAV, N., CHAUHAN, D. and GUPTA, S., 2024. CyMac: Diving Deep into the Application of Machine Learning Algorithms in Cyber Security. *International Research Journal of Innovations in Engineering and Technology,* **8**(1), pp. 74-80.
[10]DEMÓSTENES ZEGARRA RODRÍGUEZ, OKEY, O.D., MAIDIN, S.S., EKIKERE, U.U. and KLEINSCHMIDT, J.H., 2023. Attentive transformer deep learning algorithm for intrusion detection on IoT systems using automatic Xplainable feature selection. *PLoS One,* **18**(10),.
[11]DURLIK, I., MILLER, T., KOSTECKA, E., ZWIERZEWICZ, Z. and ŁOBODZIŃSKA, A., 2024. Cybersecurity in Autonomous Vehicles—Are We Ready for the Challenge? *Electronics,* **13**(13), pp. 2654.
[12]FAN, Z., LI, W., LASKEY, K.B. and KUO-CHU, C., 2024. Investigation of Phishing Susceptibility with Explainable Artificial Intelligence. *Future Internet,* **16**(1), pp. 31.
[13]GONG, R., WU, H., ZHANG, J., HUANG, Z. and YU, Z., 2024. Optimizing Transmission Line Efficiency in the Grid with Artificial Intelligence. *Journal of Electrical Systems,* **20**(9), pp. 1265-1270.
[14]GOVEA, J., GAIBOR-NARANJO, W. and VILLEGAS-CH, W., 2024. Transforming Cybersecurity into Critical Energy Infrastructure: A Study on the Effectiveness of Artificial Intelligence. *Systems,* **12**(5), pp. 165.
[15]GOVINDARAM, A. and JEGATHEESAN, A., 2024. Enhancing Industrial IoT Security: Utilizing Blockchain- Assisted Deep Federated Learning for Collaborative Intrusion Detection. *Journal of Electrical Systems,* **20**(2), pp. 1345-1363.
[16]IBRAHIM, Y.A., LEE, S. and KIM, K., 2024. Enhancing Cyber-Threat Intelligence in the Arab World: Leveraging IoC and MISP Integration. *Electronics,* **13**(13), pp. 2526.
[17]KALOGIANNIDIS, S., KALFAS, D., PAPAEVANGELOU, O., GIANNARAKIS, G. and CHATZITHEODORIDIS, F., 2024. The Role of Artificial Intelligence Technology in Predictive Risk Assessment for Business Continuity: A Case Study of Greece. *Risks,* **12**(2), pp. 19.
[18]KATRAKAZAS, P. and PAPASTERGIOU, S., 2024. A Stakeholder Needs Analysis in Cybersecurity: A Systemic Approach to Enhancing Digital Infrastructure Resilience. *Businesses,* **4**(2), pp. 225.
[19]LANKA, P., GUPTA, K. and VAROL, C., 2024. Intelligent Threat Detection—AI-Driven Analysis of Honeypot Data to Counter Cyber Threats. *Electronics,* **13**(13), pp. 2465.
[20]LI, M. and DOU, Z., 2023. Active eavesdropping detection: a novel physical layer security in wireless IoT. *EURASIP Journal on Advances in Signal Processing,* **2023**(1), pp. 119.
[21]LIGHTBODY, D., DUC-MINH NGO, TEMKO, A., MURPHY, C.C. and POPOVICI, E., 2024. Dragon_Pi: IoT Side-Channel Power Data Intrusion Detection Dataset and Unsupervised Convolutional Autoencoder for Intrusion Detection. *Future Internet,* **16**(3), pp. 88.
[22]LYSENKO, S., BOBRO, N., KORSUNOVA, K., VASYLCHYSHYN, O. and TATARCHENKO, Y., 2024. The Role of Artificial Intelligence in Cybersecurity: Automation of Protection and Detection of Threats. *Economic Affairs, suppl.Special Issue,* **69**, pp. 43-51.
[23]MOHAMED, N., 2023. Current trends in AI and ML for cybersecurity: A state-of-the-art survey. *Cogent Engineering,* **10**(2),.
[24]MOHAMMAD AFTAB, A.K. and HAZILAH, M.K., 2023. A Comprehensive Survey of Machine Learning Techniques in Next-Generation Wireless Networks and the Internet of Things. *Ingenierie des Systemes d'Information,* **28**(4), pp. 959-967.

[25]MUNEER, S., FAROOQ, U., ATHAR, A., MUHAMMAD, A.R., GHAZAL, T.M. and SAKIB, S., 2024. A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis. *Journal of Engineering,* **2024**.
[26]OLIVARES, R., SALINAS, O., RAVELO, C., SOTO, R. and CRAWFORD, B., 2024. Enhancing the Efficiency of a Cybersecurity Operations Center Using Biomimetic Algorithms Empowered by Deep Q-Learning. *Biomimetics,* **9**(6), pp. 307.
[27]ORTIZ-RUIZ, E., BERMEJO, J.R., SICILIA, J.A. and BERMEJO, J., 2024. Machine Learning Techniques for Cyberattack Prevention in IoT Systems: A Comparative Perspective of Cybersecurity and Cyberdefense in Colombia. *Electronics,* **13**(5), pp. 824.
[28]PDF, 2024. A Comprehensive Analysis of Network Security Attack Classification using Machine Learning Algorithms. *International Journal of Advanced Computer Science and Applications,* **15**(4),.
[29]PDF, 2024. Advancing Hospital Cybersecurity Through IoT-Enabled Neural Network for Human Behavior Analysis and Anomaly Detection. *International Journal of Advanced Computer Science and Applications,* **15**(5),.
[30]PDF, 2024. Botnet Detection and Incident Response in Security Operation Center (SOC): A Proposed Framework. *International Journal of Advanced Computer Science and Applications,* **15**(3),.