www.editada.org

International Journal of Combinatorial Optimization Problems and Informatics, 14(3), Sep-Dec 2023, 16-23. ISSN: 2007-1558. Doi:10.61467/2007.1558.2023.v14i3.372

Artificial Intelligence the Strategic Key of Cybersecurity

Gustavo Arroyo-Figueroa
Instituto Nacional de Electricidad y Energías Limpias
E-mail: garroyo@ineel.mx.

Abstract. Despite the fact that digital transformation introduces multiple advantages, it also introduces crucial security challenges, since it combines heterogeneous communications, the integration of digital devices, legacy technologies. In the case of power grid, in addition to damage to the availability, integrity and confidentiality of information; there may be manipulation and take control of assets through the infection of operational systems. In this context, powerful cybersecurity schemes and mechanisms that guarantee the safe transmission of information and the safe operation of assets are required. The goal is develop cyber security schemes and mechanisms based on intelligent cyber defense mechanisms that provide flexibility and self-learning capacity to support humans in the analysis and generation of containment measures against cyber-attacks. This paper presents the developed and validation of an Intrusion Detection and Prediction System (IDPS) based on individual classifiers and ensemble algorithms. The IDPS has demonstrated be an efficient countermeasure against several cyberattacks. The proposed IDPS uses J48 (decision tree), CLONAL-G (artificial immune system), bayesian classifier and ensemble algorithm and was validated with the KDDCup databases. The attacks in the data set are categorized into four attack types: DoS (denial-of-service attacks), R2L (root-to-local attacks), U2R (user-to-root attack), and Probe (probing attacks). The results show that the individual classifiers perform well for particular attack, so it was necessary to build an ensemble algorithm that combine the information from each classifier for better performance. The idea is not to rely on a single classifier for the decision, but rather individual information from different classifiers is combined to make the final decision.

Keywords: Artificial Intelligence, CyberSecurity.

Article Info
Received Jan 26, 2023
Accepted Sep 23, 2023

1 Introduction

Electricity industry, like many industries, is immersed in a process of digital transformation based on the use of emerging information technologies. The digitalization of the operational and administrative processes of the companies provides a robust platform that allows a reliable and efficient operation; proper asset management and new ways of operating and trading electricity. Some of the main elements related to the digital transformation, also known as the Industry 4.0 paradigm (Tuttokmagi & Kaygusuz, 2018), are shown in the figure 1. Emerging information and communication technologies are now the primary tools in solving the problems that arise in the areas planning, operation, diagnosis, maintenance and design of power systems.

Digital transformation includes sensors and smart devices for data collection, required to carry out process monitoring and control tasks; requires a fast Internet of Things (IoT)-based connection between smart sensors and operation systems. This is a crucial task for the correct traffic between the data and the databases of the systems; it requires integrated information systems at the different levels of the company with a high level of interoperability; powerful analytical tools for processing large volumes of information; intelligent algorithms to support operational and strategic decision-making in tasks of diagnosis, prediction, prognosis, planning and optimization of processes. Additionally, autonomous vehicles and robots for maintenance and physical security of assets and virtual reality tools for design, operation and maintenance of assets are included, see figure 1.

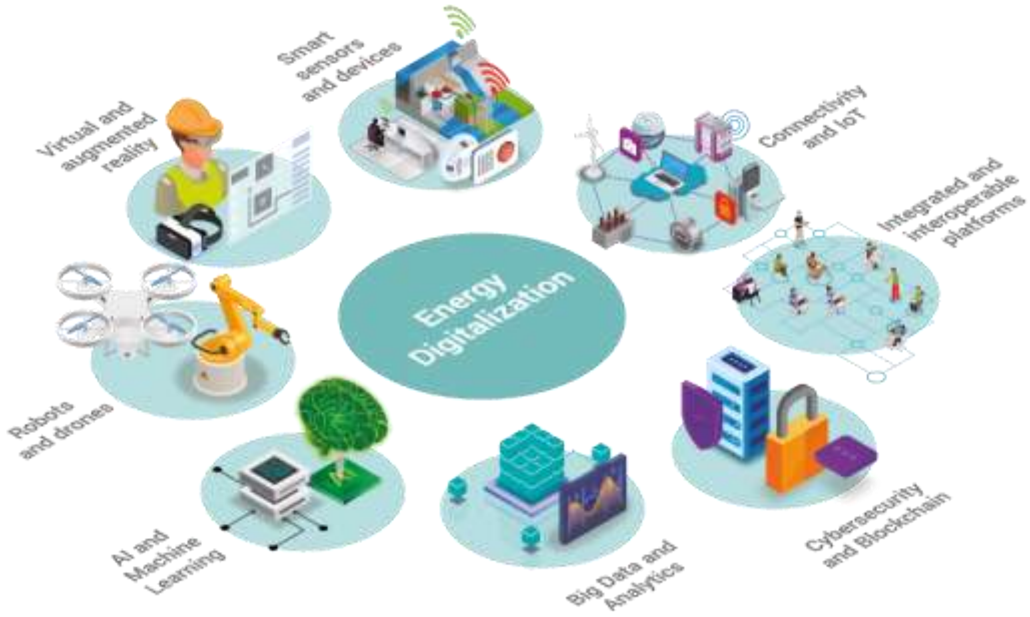

Energy Digitalization
Smart sensors and devices
Virtual and augmented reality
Connectivity and IoT
Integrated and interoperable platforms
Robots and drones
Cybersecurity and Blockchain
AI and Machine Learning
Big Data and Analytics

Figure 1. Elements of digital transformation based on emerging information technologies.

However, the digital transformation of power industry raises important questions about the security and privacy of information and assets; being an open environment with larger attack surface, including a large number of digital devices and a large number of communication nodes where there are a large number of vulnerabilities and cyber threats. Other vulnerabilities are the interconnection of corporate computer networks (RI) with operational networks (RO), where the operation and control devices are not designed and built with information security mechanisms; and the greater number and variety of users who access to information networks (Arroyo-Figueroa et al., 2020).

In this context, one of the main lines of research for power industry is the development of powerful cybersecurity schemes and mechanisms that guarantee the safe transmission of information and the safe operation of assets. It is important to mention that the case of power grid, in addition to damage to the availability, integrity and confidentiality of information; there may be manipulation and take control of assets through the infection of operational systems.

The goal is develop cyber security schemes and mechanisms based on intelligent cyber defense mechanisms that provide flexibility and self-learning capacity to support humans in the analysis and generation of containment measures against cyber-attacks. These countermeasures must be capable of managing the entire attack response process in a timely and efficient manner, that is, detecting what type of attack is occurring and what is the appropriate response, as well as how to prioritize and prevent secondary attacks or persistent.

The purpose of this work is to show the potential fields of application of intelligent cyber defense as a support tool in the context of cyber security, to show how these techniques can be an effective tool for the detection and prevention of cyber-attacks; as well as presenting the development and results of an intelligent intrusion detection and prevention system (IDPS).

2 Potential applications of AI in Cybersecurity

Artificial Intelligence (AI) is taking great interest among cybersecurity specialists. There are two main characteristics that make AI have potential applications in cybersecurity:

The ability to detect new and sophisticated attacks (Zero Day)

Conventional attack detection technology is based on data from past and known attacks, so it is limited in detecting new attacks. AI helps detect threats based on application behavior and all network activity. The intelligent security system learns about normal network behavior and traffic. The ability to adapt to detect anomalous operations faster and more accurately is especially useful as cyberattacks become more sophisticated and innovative.

The ability to handle large volumes of data

The volume of information that appears daily through the network can be very overwhelming; handling it would have great difficulties to track down and identify attack factors quickly and reliably. AI can improve network security by developing autonomous security systems capable of detecting attacks and generating countermeasure actions, using large volumes of data. Automatic detection and real-time response to threats, based on AI, will help in more effective and timely detection. In this awakening due to the use of AI in cybersecurity, four potential applications reported in the literature stand out, shown the figure 2 (Truong et al., 2020):

1. Detection of malware. Traditional methods to detect malware use a signature-based method. This method has two problems: it cannot detect new malware, and it cannot detect when obfuscation techniques are used to change the characteristics of the malware to avoid detection. AI algorithms take advantage of malware evolution for detection. AI can apply a classification algorithm based on the collected features and functions for malware detection (Aslan & Samet, 2019).
2. Intrusion detection. Intrusion detection is a cybersecurity protection technique that can intercept and respond to intrusions. An intrusion detection and prevention system (IDPS) is a system that detects when there are signs of possible incidents, violations, or imminent threats on the network based on abnormal operation. AI algorithms are appropriate for developing IDPS due to their flexibility, adaptability, learnability, and rapid response.
3. Phishing detection. Phishing is an attack method created to steal data by using emails pretending to be from well-known companies to induce people to reveal personal information, such as passwords or credit card numbers. AI techniques can detect and prevent phishing, like a typical classification task. AI AI can automatically classify email as phishing and even detect unusual activity in financial accounts. In addition, it can also prevent users from falling for domain spoofing by generating alerts when users enter spoofed websites (Sahingoz et al., 2019).
4. Advanced Persistent Threat (APT). APT is a term used to describe an attack campaign, usually by a group of attackers, using advanced attack techniques to exploit sensitive data and remain on compromised computers undetected. AI can identify and prevent APT through intrusion detection and prevention systems. Intrusions are detected early on and quickly reacted to APT in order to minimize damage. Likewise, it has the ability to differentiate between legitimate and malicious software and prevent the attack (Moon et al., 2017).

The key to using intelligent cybersecurity lies in the combination of the strengths of AI and human intelligence. Intelligent cybersecurity, also called cognitive cybersecurity, learns with every interaction to proactively detect and analyze threats, providing useful information to security analysts to make informed, timely, and accurate decisions.

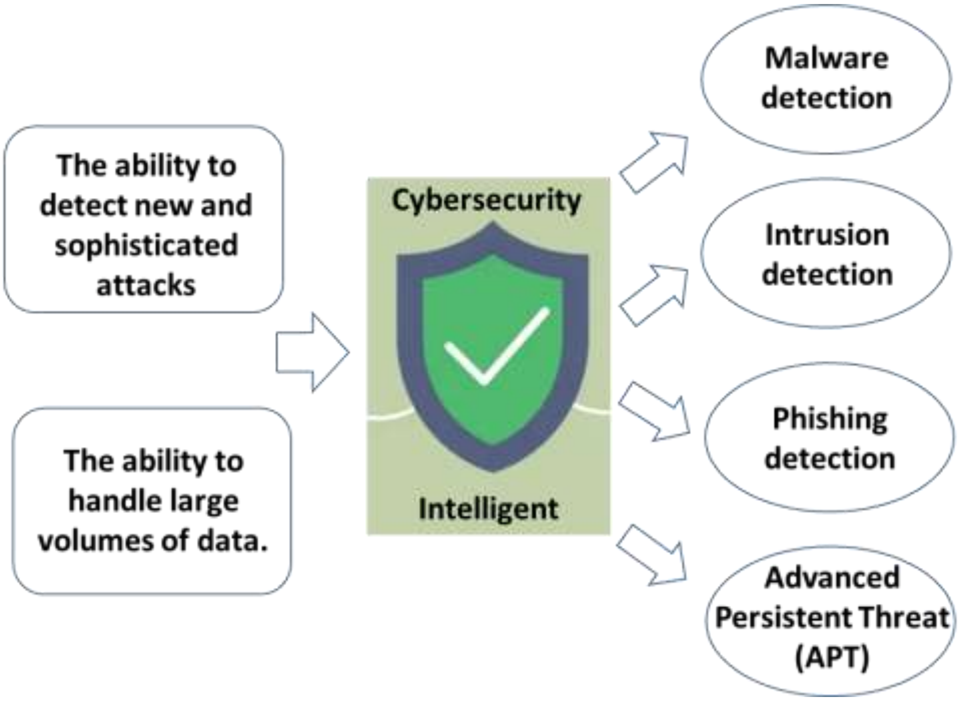

The ability to detect new and sophisticated attacks
The ability to handle large volumes of data.
Cybersecurity
Intelligent
Malware detection
Intrusion detection
Phishing detection
Advanced Persistent Threat (APT)

Figure 2. Capabilities and Potential Applications of AI in Cybersecurity

3 Intelligent Intrusion Detection and Prevention Systems (IDPS)

The most common AI applications in cybersecurity include the development of Intrusion Detection and Prevention Systems (IDPS). An IDPS can be defined as software that has the ability to detect and prevent behaviors that would indicate signs or patterns of possible intrusions. In general, IDPS fall into two categories based on the detection methods they employ:

a) Misuse detection identifies intrusions by matching observed data with predefined descriptions of intrusive behavior.
b) Anomaly detection is orthogonal to misuse detection. It is hypothesized that abnormal behavior is rare and different from normal behavior. Therefore, it builds models for normal behavior and detects anomalies in the observed data by noticing deviations from these models. There are two types of anomaly detection: static, which assumes that the behavior of monitored targets never changes, such as the system call sequences of an Apache service; and dynamic, which extracts patterns from the behavioral habits of end users or the usage history of networks/hosts. Anomaly detection has the ability to detect new types of intrusions and requires only normal data to build the patterns.

The big problem to solve is to determine the limits between normal and abnormal behavior (false positives), due to the deficiency of abnormal samples in the training phase. Another difficulty that arises is adapting to normal behavior in a constantly changing environment, especially for dynamic anomaly detection. Figure 3 shows a schematic of the 4 basic functions of an IDPS: monitor, detect, analyze and respond (Dilek, Çakır, & Aydın, 2015). An advanced IDPS additionally has a risk analysis module, an intelligent information management module and an ontology database.

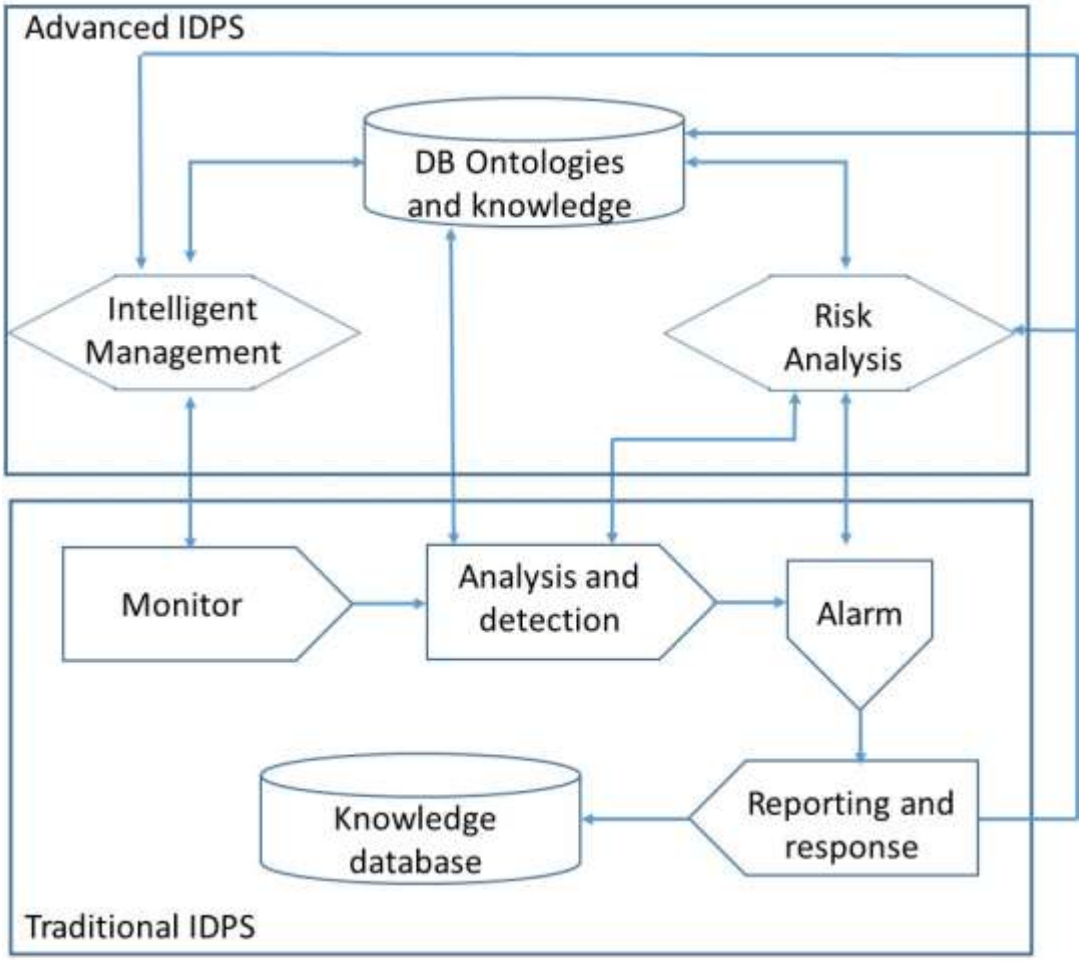


Figure 3. Traditional and advanced IDPS.

There are many AI-based IDPS reported in the literature, a brief analysis of AI algorithms used for intrusion detection is given below. An IDPS uses specific classification algorithms for each type of attack, or multiclass algorithms, which use network traffic data for intrusion detection.

The first generation of IDPS were based on known artificial intelligence techniques used for classification purpose. Patch and Park (Patcha & Park, 2007) presented a systematic survey of anomaly detection techniques proposed in 6 years from 2000 to 2006. Garcia-Teodoro et al. (2009) provided a survey of anomaly based IDSs and techniques. They classified anomaly-based detection techniques into three main categories, statistical based, knowledge based, and machine learning based. An overview of the research progress in applying computational intelligence methods to the problem of intrusion detection is presented by Wu & Banzhaf (2010). The second generation of IDS uses a Feature Selection (FS) and hybrid AI methods and ensemble AI methods. Aljawarneh et al. (2018), propose an anomaly-based intrusion detection system using feature selection analysis and a hybrid model, the building of hybrid model is based on the following classifiers: J48, Meta Pagging, Random Tree, REP Tree, AdaBoostM1, Decision Stump and Naïve Bayes. Laftah Al-Yaseen (2017) propose a multi-level hybrid intrusion detection model that uses sup- port vector machine and extreme learning machine to improve the efficiency of detecting known and unknown attacks. A good survey of intrusion detection systems based on ensemble and hybrid classifiers is presented by Aburomman & Reaz (2017).

4 IDSP development methodology.

The stages involved in the developed of the IDPS based are presented in figure 4 (Arroyo-Figueroa et al., 2020).

Database (DB). For this work, the KDD Cup '99 database was used, it contains 4,940,000 records of attacks and normal connections. The attacks in the data set are categorized into four attack types: DoS (denial-of-service attacks), R2L (root-to-local attacks), U2R (user-to-root attack), and Probe (probing attacks). The data set includes 41 features and one class (normal).

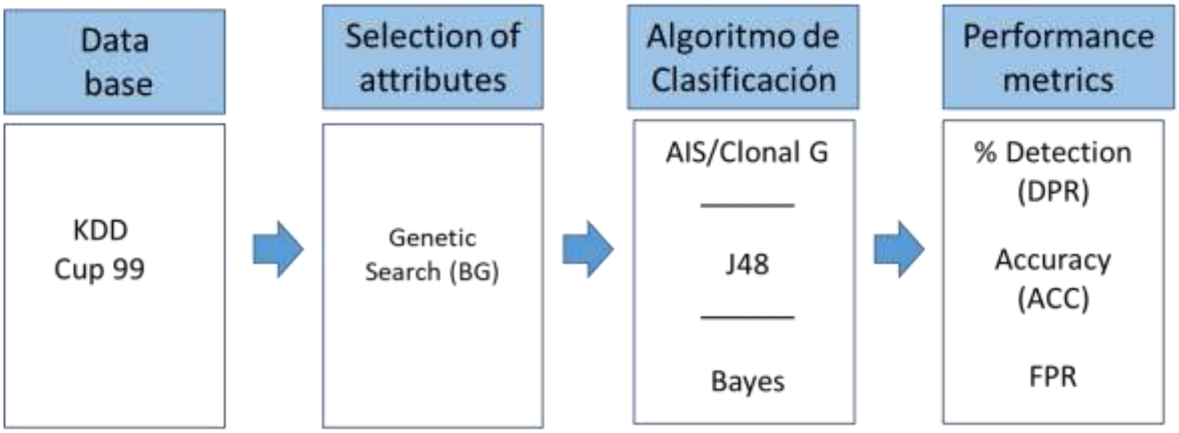


Figure 4. Framework for the development of an IDPS

Feature selection (FS). The attribute selection algorithm allows to reduce the amount of data to be processed. This is very important if real time detection is desired. FS focuses on removing redundant and irrelevant data. For this work, the genetic search attribute selection algorithm was used.

Classification algorithm. The next step is the selection of algorithm. For our case, the following classifiers were used: J48 (decision tree), CLONAL-G (artificial immune system), Bayesian classifier and ensemble algorithm.

Evaluation. The effectiveness of each classification model is evaluated by its ability to make correct predictions (% accuracy). The evaluation metrics are basically derived from the four basic attributes of the confusion matrix: true positives (TP), false positives (FP), false negatives (FN) and true negatives (TN).

5 Implementation and results

The data set contains only the 10% of the randomly generated KDD Cup99 database. The genetic search attribute selection algorithm was applied to this data set; the result was the selection of 8 attributes.

Once data is initially prepared, it is splitter into training and testing data sets. The proportions used for splitting the DB were 80% for training and 20% for testing. The classification algorithms are optimizing using GS-CV procedure. The ensemble method consists of using different training models for different base classifiers and then combining their results. The final output was defined by giving it a weight (0-1) depending on the generalization precision obtained for each classifier. If both classifiers agree, the start is decided accordingly. If there is a conflict, the decision of the classifier with the highest weight is taken into account.

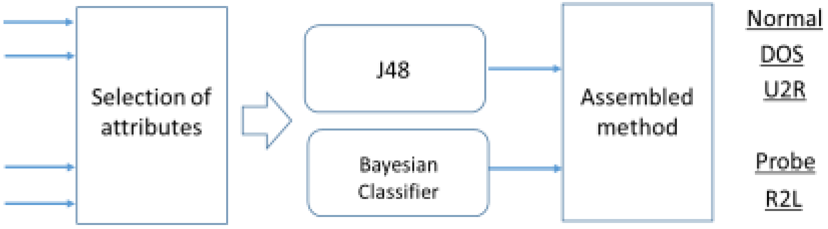
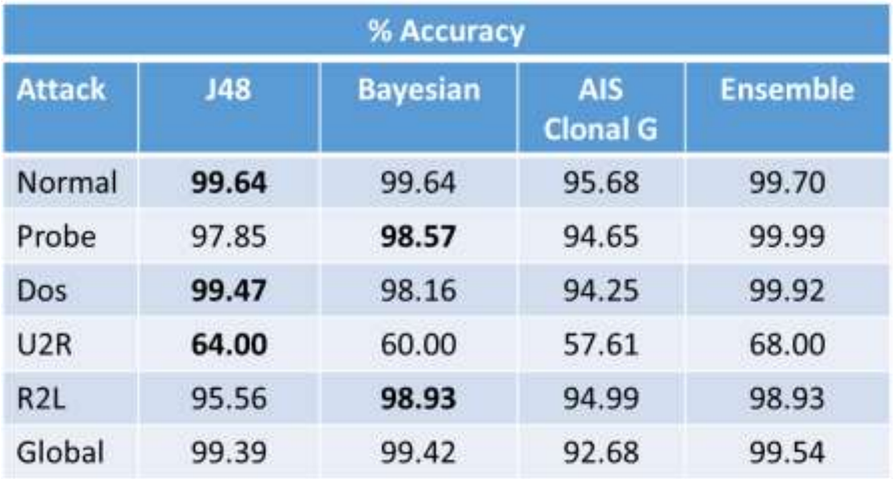


Figure 5. Implementation of the ensemble method of an IDPS.

Table 1 illustrates the results of the individual and ensemble algorithms using the same data set. The results show that the different classifiers perform well on the test. However, the algorithm that had the best performance for each attack is highlighted in black.

Table 1. Performance of the classification algorithms



% Accuracy				
Attack	J48	Bayesian	AIS Clonal G	Ensemble
Normal	**99.64**	99.64	95.68	99.70
Probe	97.85	**98.57**	94.65	99.99
Dos	**99.47**	98.16	94.25	99.92
U2R	**64.00**	60.00	57.61	68.00
R2L	95.56	**98.93**	94.99	98.93
Global	99.39	99.42	92.68	99.54

From the results, we can conclude that the ensemble method offers a better performance than the three individual models used separately. If we combine the information from each classifier, better performance will be obtained. The idea is not to rely on a single classifier for the decision, but rather individual information from different classifiers is combined to make the final decision, which is an advantage of the ensemble method.

6 Conclusions

It is important to highlight the usefulness of AI as an effective and robust support tool for cybersecurity. The large volume of data that is generated and the constant evolution of computer attacks make it essential.

Although traditionally the use of AI has been related to the construction of intelligent IDSPs, it should be noted that there are other areas of opportunity for the use of AI algorithms as a countermeasure tool against malware, phishing and ATP detection attacks.

It can be said that in general the classification algorithms present a good overall performance in the construction of IDPS, however, the same does not occur in the particular detection of each type of attack, for this reason it is necessary to use an ensemble method to generate better performance, based on the performance of individual ranking algorithms.

The area of incorporation of AI methods in cybersecurity is an area of current development, research is being carried out to generate robust and balanced attack databases; and in the development and implementation of intelligent algorithms that have the ability to anticipate attacks. There is a constant fight between the attackers and those who protec. This is undoubtedly a field of research that will continue to evolve and it will be more important every day.

References

Aburomman, A. A., & Reaz, M. B. I. (2017). A survey of intrusion detection systems based on ensemble and hybrid classifiers. *Computers & Security, 65*, 135-152.

Aljawarneha, S., Aldwairi, M., Yassein, M.B.et al. (2018). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *Journal of Computational Science, 25*, 152-160. Doi: 10.1016/j.jocs.2017.03.006

Al-Yaseen, W. L., Othman, Z.A, Ahmad Nazri, M.Z. (2017). Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system. *Expert Systems with Applications, 67*, 296-303.

Arroyo-Figueroa, G. Rojas-Gonzalez I., Hernández, J.A. (2020). A Compressive Compilation of Cyber Security for Internet of Energy (IoE). In M. D. Stojanovic & S. V. Bostjancic Rakas (Eds.), *Cyber Security of Industrial Control Systems in the Future Internet Environment* (pp. 267-294). IGI Global.

Arroyo-Figueroa, G., et al. (2020). An Intrusion Detection System for the Smart Grid based on Computational Intelligence Algorithm. *CIGRE SC D2, paper D2-206.*

Aslan, O. A., & Samet, R. (2019). A Comprehensive Review on Malware Detection Approaches. *IEEE Access, 8*, 6249-6271. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8949524

Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. *International Journal of Artificial Intelligence & Applications, 6*(1).

Garcia-Teodoro, P., Dıaz-Verdejo, J., Macia-Fernandez, G., & Vazquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security, 2*(8), 18–28.

Moon, D., Im, H., Kim, I. and Hyuk Park, J. (2017). DTB-IDS: An intrusion detection system based on decision tree using behavior analysis for preventing APT attacks. *Journal of Supercomputing, 73*(7), 2881-2895. Doi: 10.1007/s11227-015-1604-8

Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks, 51*(12), 3448–3470.

Sahingoz, O. K., Buber, E., Demir, O., Diri, B. (2019). Machine learning based phishing detection from URLs. *Expert Systems with Applications, 117*, 345-357. Doi: 10.1016/j.eswa.2018.09.029

Truong, T. C. Zelinka, I., Plucar, J., Čandík, M., Šulc, V. (2020). Artificial Intelligence and Cybersecurity: Past, Presence, and Future. In S. Dash, C. Lakshmi, S. Das, & B. Panigrahi (Eds.), *Artificial Intelligence and Evolutionary Computations in Engineering Systems. Advances in Intelligent Systems and Computing* (pp. 351-363).

Tuttokmagi, O., & Kaygusuz, A. (2018). Smart Grids and Industry 4.0. In *Proceedings of the International Conference on Artificial Intelligence and Data Processing* (pp. 1-6).

Wu, S. X., & Banzhaf, W. (2010). The Use of Computational Intelligence in Intrusion Detection Systems: A Review. *Applied Soft Computing, 10*, 1-35.