BULETINUL INSTITUTULUI POLITEHNIC DIN IAŞI
Publicat de
Universitatea Tehnică „Gheorghe Asachi” din Iaşi
Volumul 65 (69), Numărul 2, 2019
Secția
ELECTROTEHNICĂ. ENERGETICĂ. ELECTRONICĂ

USING ARTIFICIAL INTELLIGENCE AND SEMANTIC WEB TECHNOLOGIES INSIDE CYBERDEFENSE SYSTEMS

BY

ANDREI ZAMFIRA[1,*], RALUCA FĂT[2] and CĂLIN CENAN[2]

[1]Politehnica University of Timişoara,
Department of Computer Science,
[2]Technical University of Cluj-Napoca,
Department of Automation and System Engineering

Received: December 27, 2018
Accepted for publication: April 15, 2019

Abstract. In this paper we will make a study and analyses regarding the new techniques used in the construction of Intrusion Detection Systems (IDS). Because most of these techniques, as it is stated in the literature, come from the Artificial Intelligence domain, here we will focus our attention also on it, more specifically Machine Learning. Are discussed some of the most important techniques from this domain and it is shown how they can be used to improve the detection of attacks. Models in the form of UML diagrams are presented with the scope to also visually illustrate the role of each technique in the intrusion detection process. From the articles studied in the literature by authors in conducting the current research was compiled a list of some commercial/research IDS products that use Machine Learning algorithms in their detection methodologies. Like in any review paper, the reader is provided with references in literature where one can find more information to enrich its knowledge for the particular discussed domain.

Keywords: artificial intelligence; machine learning; deep learning; semantic web; intrusion detection system; intelligent technology.

[*]Corresponding author: *e-mail*: andreizamfira@gmail.com

1. Introduction

Intrusion Detection is the process of monitoring events occurring in a computer system or network and their analysis to discover possible signs of incidents, such as violations of security policies of computers, acceptable usage policies, or standard security practices. The incidents can have multiple forms, such as malware (worms, spies, viruses), attackers get unauthorized access to systems and resources, authorized users of systems that misuse their privileges or try to obtain others (McMorrow, 2010).

Intrusion Detection Systems (IDS) are security tools that, like other measures such as antiviruses, firewalls, control access schemes, have the goal to strengthen the informational security of different computing and communication systems. Intrusion Prevention Systems (IPS) is a software tool that has all capabilities of an IDS and also attempts to stop the detected incidents by means of some prevention mechanisms. IDS and IPS technologies share many capabilities, and administrators can choose to disable prevention of IPSs making them to work as IDSs. In this paper we will use the term 'IDPS' as a shorthand to refer to both technologies (Mell & Scarfone, 2007).

An important attribute of IDPS technologies is that they cannot provide completely accurate detection. In this context can be remarked four situations corresponding to relations between detection results of an event and its real nature (malicious/inocuous):

– false positive (FP): analyzed event is clear from security perspective but is misclassified as attack;

– true positive (TP): analyzed event is correctly classified as attack;

– false negative (FN): analyzed event is an attack but is misclassified as normal;

– true negative (TN): analyzed event is correctly classified as normal.

It can be observed that low rates of FP and FN, together with high rates of TP and TN will result in a good and efficient detection.

Depending on the information source considered, an IDPS can be for Host or Network. A host IDPS (HIDS) analyzes events such as process identifiers and system calls, especially related to OS operation. A network IDPS (NIDS) analyze events from the networks, such as traffic volume, IP addresses, ports in service, protocol usage, bandwidth consumption, and many other traits.

The main detection methodologies employed by IDPS systems are (Agarwal & Hussain, 2018):

– signatures-based;

– anomaly-based;

– stateful protocol analysis.

Signature-based (or misuse) schemes compare the signatures of known attacks against the observed events to identify possible signs of intrusions. Anomaly-based schemes compare the definition of activity that is considered normal against observed events to identify significant deviations. An IDPS that

uses this detection technique has profiles of normal behavior of staff like users, hosts, networks, connections, applications. Profiles are created by monitoring the characteristics of typical activities on a period of time. The third methodology, State Protocol Analysis (SPA), is somehow related to the anomaly one, in the way that it compares the predefined profiles of activities for benign profiles for each state of the protocol, against the observed events on the network to identify deviations. Unlike anomaly-based though, that uses specific profiles of hosts or networks, SPA relies on universal profiles that were created by vendors that specify how/not the products should be used.

In this paper we will consider only the second methodology, that of anomaly-based. The advantage of this technique is that it is able to detect incidents unknown before (zero-day). Despite their inaccuracy in formal specification of signatures, false positive rates are generally higher than in signatures technique. Given the promising capabilities of anomaly-based detection systems (A-NIDS), this is now an important area of research and development in intrusion detection. Various systems with A-NIDS capabilities have become available and many new schemes were explored, with all that the subject is far from its maturity and problems remain unsolved before the large scale deployment of A-NIDS platforms to be a practical thing (Garcia-Teodoro *et al*., 2009).

2. Artificial Intelligence and Machine Learning in Cybersecurity

Artificial Intelligence (AI) is a computer discipline which has the main goal to simulate the human intelligence processes by using machines. Their 'fathers' are considered to be Alan Turing and John McCarthy. The former published in 1950 a landmark paper in which he sustained the idea of creating machines that could think similarly as humans do. He affirmed that 'thinking is a process difficult to define' and proposed his famous Turing Test (Turing, 1950). The latter coined the term at a conference in Dartmouth, 1956. As the term suggests, intelligence is 'artificial' and is programmed by humans into machines to make them perform human-like tasks and tries to best approximate human intelligence (Wu, 2019). Two of its most important branches are Machine Learning and Deep Learning, as it is showed in Fig. 1.

The definition of Machine Learning (ML), as given by one of its pioneers, Arthur Samuel, from 1959 says: 'a field of study that focuses on giving computers the ability to learn without being explicitly programmed'. The learning is a five-step process, as it is shown in (Rouse, 2018) and relies on establishing an implicit or explicit model by means of which the analyzed patterns are classified and categorized. Its algorithms fall into 3 main classes of learning: supervised, unsupervised and reinforcement.

Deep Learning is the next-gen development of the ML technologies. Deep Learning models rely on Artificial Neural Networks (ANN) to make their own predictions entirely independent of humans, unlike ML, which still needs

human intervention to arrive at the destination. The design of Artificial Neural Networks is inspired by the biological structure of the human brain, featuring neurons and synapses between them. ANNs analyze data with a logical structure similar to how a human draws conclusions (Wu, 2018).

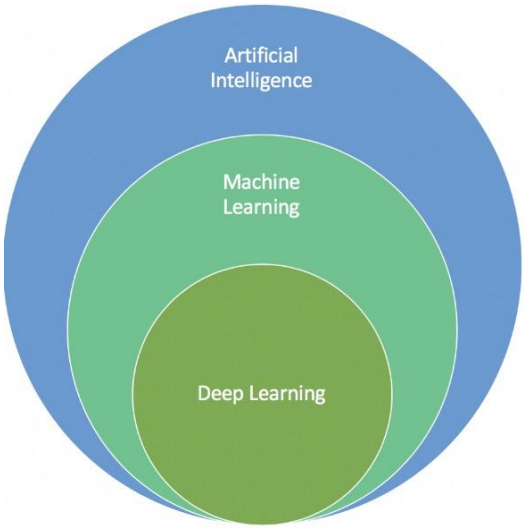

Fig. 1 – The location of major sub-fields of AI: Machine and Deep Learning.

In continuation of this section we will present the main ML algorithms that have been used in Cybersecurity and name a few industrial-scale systems who employ those techniques in the detection methodology. We will not enter into details regarding definitions and characteristics of each of the ML techniques since this is outside the scope of current work, but give readers references in literature where they can find more information.

Evolutionary Computing (EC) is a class of Machine Learning algorithms for global optimization problems inspired by biological evolution of living organisms (Nicholson, 2017). Their goal is to find optimal solutions to problems, thus finding application in many domains from mathematics and computer science. The most important technologies that form this class are: Genetic Algorithms (GA), Genetic Programming (GP) and Grammatical Evolution (GE) (Michalewicz *et al.*, 1997). The areas from intrusion detection where GA had been mostly employed are: automatic model design, classification, optimization feature selection. The main benefits that these techniques brought to the field, as it was said in (Majeed & Kumar, 2014) are:

i) provide an intrinsic parallelism, making them suitable for analyzing high volumes of data necessary in detection situations;

ii) are suitable for behavior-based intrusion detection because they work with populations of solutions;

iii) increase the adaptability of the system due to the fact that they are highly re-trainable;

iv) help in dynamic rule generation due to the property of evolving in time.

According to (Abdullad *et al*., 2009), the role of GAs is to derive a set of classification rules from network audit data and the support-confidence framework is utilized as fitness function to assess the quality of each rule. Generated rules are then used to detect/classify events from real environment networks. This process model is shown in Fig. 2. Another work, (Ganapathy *et al*., 2013) employed GA to select significant features from the test dataset, KDDCup99, in order to conduct a better analysis of events in networks.

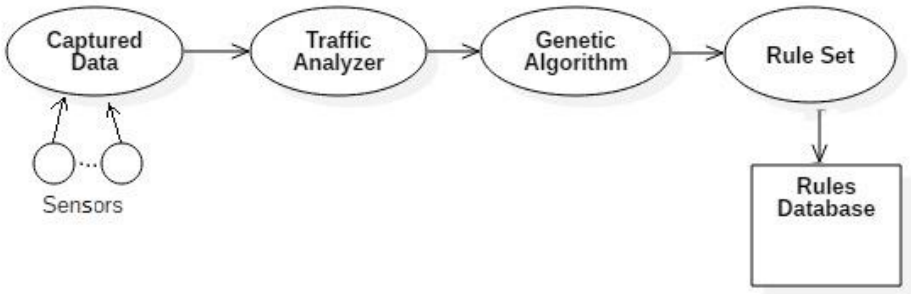

Fig. 2 – The location of the GA module within an IDPS.

The second major EC technique, Genetic Programming, was proven to be very useful in the domain, same as Gas. LaRoche & Heywood, (2005), discussed the use of GP for attack detection in 802.11 networks and stated what causes the reduction of GP's detection rate when facing attacks specific to the 802.11 protocol. One of the greatest research systems developed by now that relies on evolutionary computing is ECJ27, a Java-based Evolutionary Computation research system, described by some as "the most widely-used general purpose evolutionary computation library" that was used also in creation of cyber defense systems.

Fuzzy Logic is a superset of the traditional (Boolean) logic that was extended with multiple values of truth in order to be able to represent imprecision and uncertainty associated with behaviors from real world , also called *multivalued logic* (Elkan, 2009). In computer security, fuzzy logic is a major technique that is used in analysis. Fuzzy systems are characterized by their abilities to reason over incomplete or uncertain data, which makes them good tools for risk evaluation and analysis. Ansari *et al*., (2007), proposed the use of fuzzy logic in generating discovery rules of Data Mining to incorporate cognitive aspects to support FRCP amendments. Alali *et al*., (2018), proposed an inference system based on fuzzy rules for better assessing the risk of attacks in cybersecurity. Fuzzy methods are used in the field of anomaly-based intrusion detection mainly because the features to be considered can be seen as fuzzy variables from the set. They proved to be efficient especially against port

scans and probes. The major drawback is the high resource requirements for processing (Thakare & Ali, 2012).

Cluster analysis and outliers is an unsupervised ML technique that involves grouping (or classification) of a set of data points into a specific group according to a similarity (distance) metric. For a brief introduction and a list of the most important algorithms developed in this field reader is invited to see Seif, (2018). Clustering and outliers are currently mostly used in the anomaly-based detection, where isolated outliers are seen as anomalies. The benefit they bring is that the effort required to tune the IDS is small since this technique determines the occurrence of intrusion events only from the raw audit data. The model of detector based on clustering and outliers is shown in Fig. 3. Brahmi *et al*., (2018), presents the work for developing an intrusion detection system that employs AI technologies of ontologies and multi-agents and proposes a clustering algorithm with the goal of increasing the scalability and detection ability of the system. One of the vastest works read by author is Agarwal & Hussain, (2018), that is both a comprehensive review of the domain and also a contribution with a conceptual framework of an 'ideal' web-based IDS that employs many technologies, some from the AI.

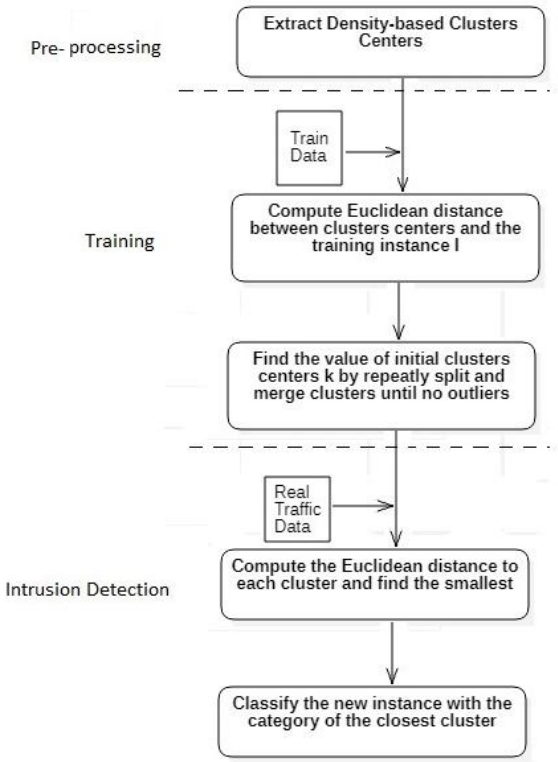

Fig. 3 – The clustering and outliers-based intrusion detection process.

Artificial Neural Networks (NNs, or ANNs) is a mathematical model that deals with information in a way inspired by the functionality of the biological nervous system (Nicholson, 2017). Lee, (2018) presents the most important 10 types of ANN architectures that were created by present day. This technology can find applications in many domains due to their abilities to make accurate decisions and recognize patterns, and represent the core component of Deep Learning. ANNs are used especially in anomaly-based detection to create and learn profiles of benign behaviors from raw audit traffic data and to detect by classifying new events based on the established profiles (Sani *et al*., 2009). The conceptual model of the process is presented in Fig. 4. In Al-Janabi *et al*., (2011), is proposed an IDS that relies on ANNs for the detection and classification of attacks in computer networks and states that this approach is superior to the traditional signature-based because is capable to learn the dynamical changing behaviors of users and systems and also has a great adaptability to changes, the drawback is the training phase that is time consuming. Paper of Igor *et al*., (2014), is a study related to the advantages of using ANNs in anomaly intrusion detection systems.

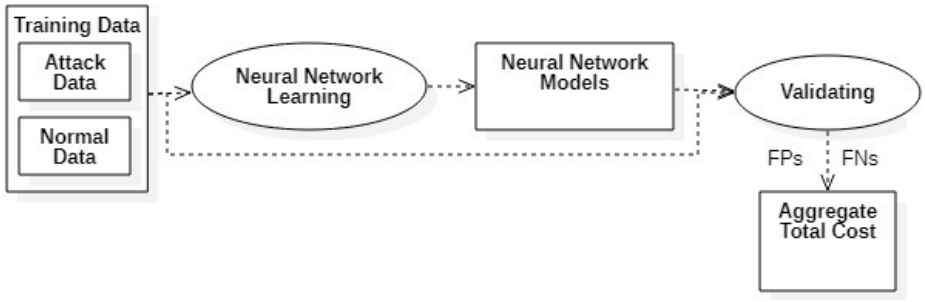

Fig. 4 – Use of ANNs in attack detection.

Data Mining (DM) is a technique for sorting through large datasets to identify new patterns and hidden information and establish relations to solve problems by data analysis, allowing to predict future trends; it is seen as a more specialized form of Knowledge Discovery in Data (Fayyad *et al*., 1996). For the most important DM methods readers are suggested to see the reference from site (educba.com, 2017) in the references section. Data Mining techniques can be very useful in intrusion detection since attacks detection involve analysis of high data volumes.

Data Mining's role in attacks detection is mainly that of data analysis, more specifically is focused on dimensionality reduction, clustering and classification, as it is shown in Fig. 5. Brahmi *et al*., (2010), affirmed that the application of Data Mining techniques in intrusion detection can improve detection accuracy, speed and enhance system's own security. They proposed a distributed IDS that uses the AI technologies of multi-agents, data mining and clustering to overcome the above stated problems. Others affirmed that the

advantage over signature-based intrusion detection is the high degree of accuracy in detecting in detecting known attacks and their variations (Lazarevic *et al*., 2005).

The five techniques presented in this section are not the only AI technologies that are being used in cyberdefense, but are definitely the most important. For other technologies we invite the reader to see the works of (Garcia-Teodoro *et al*., 2009; Tsai *et al*., 2009; Banoth *et al*., 2017; Bankovic, 2007) where other ML techniques are described together with their application in cyber-security field.

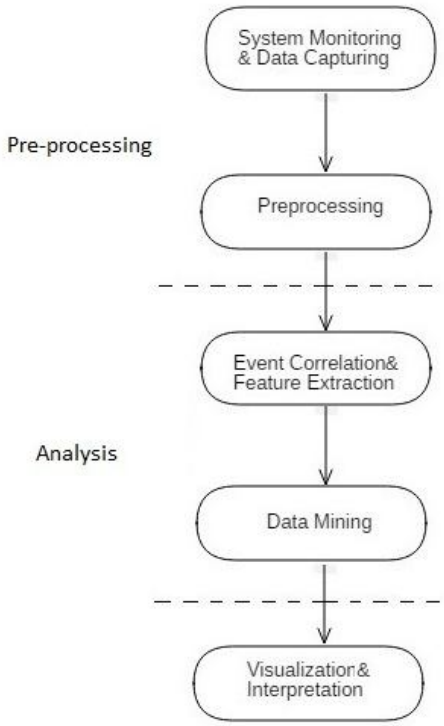

Fig. 5 – Data Mining's role in the process of intrusion detection.

Table 1 presents a survey with some of the research products that employ AI techniques in their detection methods, from the domain literature that was read by the author in conducting the current research. Other such lists of commercial tools can be found in the works of (Lazarevic *et al*., 2005; Garcia-Teodoro, 1999; Jackson, 1999).

For a list of state-of-art commercial NIDS relying on AI and ML technologies in their detection to be seen the recent articles from the renown American company specialized on business research and analysis, Aite Group (Knight, 2019a,b; Knight, 2018a,b).

Table 1
List of Some NIDS Commercial Products and ML Techniques Employed

NIDS Product	Owning organization	AI methods employed
EMERALD (Event Monitoring Enabling Response to Anomalous Live Disturbance)	SRI International	Rule-based expert systems, Bayesian inference, forward chaining
NetSTAT (Network-based State Transition Analysis Tool)	University of California Santa Barbara	State-transition analysis rules
Bro	Lawrence Livermore National Laboratory	Application-level semantic, Pattern matching
ComputerWatch	Secure Systems Dept, AT&T Communicat.	Expert systems, Pattern matching, rule-based
AAFID (Architecture for Intrusion Detection using Autonomous Agents)	Purdue University	Autonomous agents
Hummer	University of Idaho	Data mining, Autonomous agents
JAM (Java Agents for Meta-learning)	Columbia University	Neural Networks training, Naïve Bayes classifier, Data mining, Nearest Neighbor, Decision Tree, Rule-based inference
Snort IDS	Cisco Systems	Statistical analysis
MINDS (Minnesota Intrusion Detection System)	University of Minnesota	Data Mining, Pattern matching, Clustering and outliers
DMNIDS (Data Mining for Network Intrusion Detection Systems)	MITRE corporation	Data Mining, Clustering and outliers
MADAM	Columbia University	Data Mining, Association rules, Frequent episodes

3. Semantic Web in Intrusion Detection

Semantic Web, as it was affirmed by its inventor Tim Berners-Lee, is the vision of a fully automated Web of machines that communicate and carry out tasks instead of humans, programs that manipulate things meaningfully, data that have a universal structure and format in order to be comprehensible by machines (Berners-Lee *et al*., 1999).

Semantic Web techniques of “content” and “ontology” can be used in many areas of the Computer Science. Each security approach that uses the concept of “content” can use methods and techniques from Semantic Web, and the intrusion detection systems are a good example (Abdoli&Kahani, 2009).

Even though IDSs are a main component of the security infrastructures, they suffer from a number of problems, most important are: reliability, relevance, disparity and incompleteness in the presentation and manipulation of knowledge and detection of attacks.

Most IDSs have a centralized architecture which uses multiple generic nodes that communicate with a central processing node. This approach suffers from the problem of the 'single point of failure', that is, whenever the central node is attacked the entire IDS is put at risk. Also the transfer of all the information to a single node puts great demands on network resources and leads to network overload. One solution to the above problems is the integration of a multi-agents technology within the IDS. The use of multi-agent techniques in intrusion detection offers a series of advantages, like scalability, minimal network overhead, independent and continuously running of agents etc, making the resilience of the system strong and ensuring its safety (Brahmi *et al*., 2011).

Alongside, the concept of 'ontology' has emerged as a technique for representation and sharing the knowledge of a domain. In the intrusion detection field, ontologies are used to give IDSs the ability to share a common understanding about intrusions and design the signatures rules. The use of ontologies in intrusion detection domain has the following advantages, as it was stated in (Abdoli & Kahani, 2009):

– grasps semantic knowledge of the domain;

– better expresses the IDS by building better rules of signatures using specific Semantic Web languages (*e.g*. RIF, SWRL);

– makes the reasoning an intelligent process.

Some computer scientists have opened a new branch in the informational security, that of using ontologies with their advantages. They said that "ontologies are an extremely promising new paradigm in the field of computers security by means of which we have a classification tool of unlimited events" (Razzaq *et al*., 2014).

The use of Semantic Web technologies in the construction of intrusion detection systems is a new concept. Among the first researches in this field were those of (Undercoffer *et al*., 2003a,b). In one of them, they developed an ontology that represents a model of computer attacks and affirmed that any taxonomical characteristic used for defining a computer attack must be limited in scope to those features observable and measurable at the target. The second work presents an ontology that defines relations between features that are observable by IDS sensors.

4. Conclusion

The main objective of this paper was to present and explain different methods and techniques that are used in intrusion detection field in order to build more performant, robust, intelligent systems with improved functionalities.

The currently existing platforms can be split into two categories: available commercial and research systems. Commercial systems tend to use well-proven techniques, mostly relying on signature modules. Research systems are those who embed the most recent and innovative approaches, such as ones from AI and SW that we presented here. We chose the domain of Artificial Intelligence and the newly occurred Semantic Web, since these are most widely used technologies in building intelligent and capable systems in every industry, and Cybersecurity is a good example. For each technology is briefly explained the role it has in intrusion detection, as it was stated by various works from literature read by authors in conducting the current research. Also are presented the industrial scale systems that employ those techniques in their detection methodologies.

REFERENCES

Abdoli F., Kahani M., *Ontology-Based Distributed Intrusion Detection System*, Proceedings of 14th International Computer Conference (CSICC), Teheran, Iran, 2009.

Abdullah B., Abd-Alghafar I., Salama G., *Performance Evaluation of a Genetic Algorithm-based Approach to Network Intrusion Detection System*, Proceedings of 13th International Conference on Aerospace Sciences and Aviation Technology (ASAT), Cairo, Egypt, 2009.

Agarwal N., Hussain Z., *A Closer Look at Intrusion Detection Systems for Web Applications*, Hindawi Journal on Security and Communication Networks, 2018.

Alali M., Almogren A., Hasan M., Rassan I., Bhuyian A., *Improving Risk Assessment Model of Cyber Security Using Fuzzy Logic Inference System*, Computers & Security, **74**, Elsevier (2018).

Al-Amro S., Elizondo D., Solanas A., *Evolutionary Computation in Computer Security and Forensics: An Overview*, Computational Intelligence for Privacy and Security, **1**, 25-34 (2012).

Alhazzaa L., *Intrusion Detection Systems using Genetic Algorithms*, Technical Report, King Saudi University, 2002.

Al-Janabi S., Amjed-Saced H., *A Neural Network-based Anomaly Intrusion Detection System*, Proceedings of 4th International Conference on Developments in eSystems Engineering, Dubai, UAE, 2011.

Alton L., *The Seven Most Important Data Mining Techniques*, https://www.data sciencecentral.com/profiles/blogs/the-7-most-important-data-mining-techniques, 2017.

Ansari A., Patki T., Patki A., Kumar V., *Integrating Fuzzy Logic and Data Mining: Impact on Cybersecurity*, Proceedings of 4th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Haikou, China, 2007.

Bankovic Z., Stepanovic D., Bojanic S., Taladriz O., *Improving Network Security Using Genetic Algorithms Approach*, Computers&Electrical Engineering, **33**, *5-6*, Elsevier Journal (2007).

Banoth L., Teja M., Saicharan M., Chandra N., *A Survey of Data Mining and Machine Learning Methods for Cyber-Security Intrusion Detection*, International Journal of Research, **4**, *5* (2017).

Barnett V., Lewis T., *Outliers in Statistical Data*, ISBN: 978-0-471-93094-5, Wiley, 1994.

Berners-Lee T., Hendler J., Lasilla O., *The Semantic Web*, Scientific American Magazine, feature article (2001).

Brahmi I., Brahmi H., Yahia S., *A Multi-agents Intrusion Detection System Using Ontology and Clustering Techniques*, HAL Inria, 2018.

Brahmi I., Yahia S., Aouadi H., Poncelet P., *Towards a Multi-Agent Based Intrusion Detection System Using Data Mining Approaches*, Proceedings of 7th International Workshop on Agents and Data Mining Interaction (ADMI), 173-194, Taipei,Taiwan, 2011.

Breunig M., Kriegel H., Ng R., Sander J., *LOF: Identifying Density-Based Local Outliers*, Proceedings of the National Information Systems Security Conference, 2000.

Buji A., *Genetic Algorithms for Tightening Security*, Master Thesis, University of Oslo, Oslo, Norway, 2017.

Chapke P., Deshmukh R., *Intrusion Detection System using Fuzzy Logic and Data Mining Techniques*, Proceedings of International Conference on Advanced Research in Computer Science Engineering and Technology (ARCSET), Unnao, India, 2015.

Crosbie M., Spafford E., *Applying Genetic Programming to Intrusion Detection*, Proceedings of Association of Advanced Artificial Intelligence (AAAI), Fall Symposium on Genetic Programming, Cambridge, UK, 1-8 (1995).

Drolet M., *The Darwin Defense: can Genetic Algorithms outsmart malware?*, https://www.csoonline.com/article/3237671/the-darwin-defense-can-genetic-algorithms-outsmart-malware.html, 2017.

Elkan C., *Fuzzy Logic Tutorial: What is, Applications and Examples*, https://www.guru99.com/what-is-fuzzy-logic.html, 2006.

Fayadd U., Piatetsky-Shapiro G., Smith P., *From Data Mining to Knowledge Discovery in Databases*, AAAI Journal, **17**, *3* (1996).

Fouad N., Hameed S., *Genetic Algorithm-based Clustering for Intrusion Detection*, Iraqi Journal of Science, **58**, *2*, 929-938 (2017).

Ganapathy S., Kulothungan K., Muthurajkumar S., Vijayalakshmi M., Yogesh P., *Intelligent Feature Selection and Classification for Intrusion Detection in Networks: A Survey*, EURASIP Journal on Wireless Communications and Networking (2013).

Garcia-Teodoro P., Diaz-Verdejo J., Macia-Fernandez G., Vazquez E., *Anomaly-Based Network Intrusion Detection: Techniques, Systems, Challenges*, Computers and Security, **28**, 18-28, Elsevier (2009).

Heckerman D., *A Tutorial on Learning with Bayesian Networks*, Microsoft Research Technical Report MSRTR-95-06, 2008.

Hernandez-Castro J., Isasi P., *Evolutionary Computation in Computer Security and Criptography*, New Generation Computing, 23, Springer (2005).

Hoffmann A., *Artificial and Natural Computation*, International Encyclopedia of the Social and Behavioral Sciences, 27-31, Elsevier, 2015.

Igor H., Bohuslava J., Martin J., Martin N., *Application of Neural Networks in Computer Security*, 24th International Symposium on Intelligent Manufacturing and Automation, Zadar, Croatia, 2013.

Jackson K., *Intrusion Detection Systems Product Survey*, Los Alamos National Laboratory Research Report, LA-UR-99-3883, New Mexico, USA, 1999.

Kaliapan J., *Intrusion Detection using Artificial Neural Networks with Best Set of Features*, International Arab Journal of Information Technology, **12**, *6* (2015).

Karande H., P.Kulkarni H., Gupta S., Gupta D., *Security Against Web Application Attacks Using Ontology-Based Intrusion Detection System*, International Research Journal of Engineering and Technology (IRJET), **3** (2016).

Khairkar A., *Intrusion Detection System Based on Ontology for Web Applications"*, College of Engineering, Pune, 2013.

Knight A., *A Cylance Case Study: Machine Learning in Insider Threat Incident Response*, https://www.aitegroup.com/report/cylance-case-study-machine-learning-insider-threat-incident-response, Aite Group, 2018.

Knight A., *A Darktrace Case Study: ML Rising*, Aite Group, 2018, https://www.aitegroup.com/report/darktrace-case-study-ml-rising.

Knight A., *The Titans of AI and ML Arms Race in Cybersecurity*, Aite Group, 2019 https://www.aitegroup.com/report/titans-ai-and-ml-arms-race-cybersecurity..

Knight A., *Top 10 Trends in Cybersecurity, 2019: User Experience and Machine Learning*, https://www.aitegroup.com/report/top-10-trends-cybersecurity-2019-user-experience-and-machine-learning, Aite Group, 2019.

Kumar G., Kumar K., Sachdeva M., *The Use of Artificial Intelligence-Based Techniques for Intrusion Detection: A Review*, Artificial Intelligence Review, **34**, *4*, Springer (2010).

LaRoche P., Heywood A., *802.11 Network Intrusion Detection Using Genetic Programming*, Proceedings of 7th Workshp on Genetic and Evolutionary Computation (GECCO), 170-171, Washington DC, USA, 2005.

Lazarev A., Kumar V., Srivastava J., *Intrusion Detection Systems: A Survey*, Managing Cyber Threats. Massive Computing, **5**, Springer, Boston MA (2005).

Lee J., *A Gentle Introduction to Neural Networks for Machine Learning*, https://www.codementor.io/james_aka_yale/a-gentle-introduction-to-neural-networks-for-machine-learning-hkijvz7lp, 2018.

Majeed P., Kumar S., *Genetic Algorithms in Intrusion Detection: A Survey*, International Journal of Innovation and Applied Sciences (IJIAS), **5**, *3* (2014).

Marinescu D., *Nature-Inspired Algorithms and Systems*, Complex Systems and Clouds, 33-63, Elsevier, 2017.

McMorrow D., *Science of Cybersecurity*, JASON Project, The Mitre Corporation, McLean, Virginia, 2010.

Michalewicz Z., Michalewicz M., *Evolutionary Computation Techniques and their Applications*, IEEE International Conference on Intelligent Processing Systems (ICIPS), Beijing, China, 1997.

Mkuzangwe N., Nelwamondo F., *A Fuzzy Logic-based Network Intrusion Detection System for Predicting the TCP SYN Flooding Attack*, Proceedings of 9th International Asian Conference on Intelligent Information and Database Systems (ACIIDS), 14-22, Kanazawa, Japan, 2017.

Nicholson C., *A Beginner's Guide to Evolutionary and Genetic Algorithms*, AI Wiki, https://skymind.ai/wiki/evolutionary-genetic-algorithm, 2017.

Nicholson C., *A Beginner's Guide to Neural Networks and Deep Learning*, AI Wiki, https://skymind.ai/wiki/neural-network, 2017.

Parveen J., *Neural Networks in Cybersecurity*, International Research Journal on Computer Science (IRJCS), **4**, *9* (2017).

Razzaq A., Anwar Z., Ahmad F., Latif K., Munir F., *Ontology for Attack Detection: An Intelligent Approach to Web Application Security*, Computers & Security, **45**, Elsevier (2014).

Razzaq A., Farooq A.H., Haider N., *Ontology-based Application-level Intrusion Detection System Using Bayesian Filter*, Proceedings of 2nd International Conference on Computer, Control and Communication (IC4), Karachi, Sindh, Pakistan, 2009.

Rouse M., *What is Machine Learning?*, https://searchenterpriseai.techtarget.com/definition/machine-learning-ML, 2018.

Sani Y., Mohamedou A., Ali K., *An Overview of Neural Networks Use in Anomaly Intrusion Detection Systems*, Proceedings of 7th IEEE Student Conference on Research and Development (SCORED), Serdang, Malaysia, 2009.

Scarfone K., Mell P., *Guide to Intrusion Detection and Prevention Systems(IDPS)*, Recommendations of the National Institute of Standards and Technology (NIST), Special Publication, 2007.

Seif G., *The Five Clustering Algorithms Data Scientists Need to Know*, https://towardsdatascience.com/the-5-clustering-algorithms-data-scientists-need-to-know-a36d136ef68, 2018.

Sequeira K., Zaki M., *ADMIT: Anomaly-Based Data Mining for Intrusions*, Proceedings of 8th ACM SIGKDD International Conference, 2002.

Shanmugavadivu R., *Network Intrusion Detection System Using Fuzzy Logic*, Indian Journal of Computer Science and Engineering (IJCSE), **2**, *1* (2014).

Sinclair C., Pierce L., Matzner S., *An Application of Machine Learning to Network Intrusion Detection*, Proceedings of 15th Annual Computer Security Applications Conference (ACSA), Phoenix, Arizona, 1999.

Thakare S., Ali M., *Introducing Fuzzy Logic in Network Intrusion Detection*, Journal IJARCS, **3**, *3* (2012).

Tianfield H., *Data Mining-based Cyber Attacks Detection*, System Simulation Technology, **13**, *2* (2017).

Tsai C., Hsu Y., Lin C., Lin W., *Intrusion Detection by Machine Learning: A Review*, Expert Systems with Applications, **36**, 11994-120000, Elsevier (2009).

Turing A.M., *Computing Machinery and Intelligence*, Mind Journal, Oxford University Press (1950).

Undercoffer J., Joshi A., Pinkston J., *A Target-centric Ontology for Intrusion Detection*, *18th* International Joint Conference on Artificial Intelligence, Acapulco, Mexico, 2003.

Undercoffer J., Joshi A., Pinkston J., *Modeling Computer Attacks: An Ontology for Intrusion Detection*, 6th International Symposium Recent Advances in Intrusion Detection, Pittsburgh, PA, 2003.

Wu J., *Artificial Intelligence, Machine Learning and Deep Learning Explained Simply*, https://towardsdatascience.com/ai-machine-learning-deep-learning-explained-simply-7b553da5b960, 2019.

* * * *Data Mining Methods*, https://www.educba.com/data-mining-methods/, 2017.

UTILIZAREA TEHNOLOGIILOR DE INTELIGENȚĂ ARTIFICIALĂ ŞI WEB SEMANTIC ÎN CREAREA SISTEMELOR DE SECURITATE CIBERNETICĂ

(Rezumat)

În această lucrare vom face un studiu şi o serie de analize a noilor tehnologii folosite la construirea sistemelor de detecție a intruziunilor (IDS). Deoarece marea parte

a acestor tehnologii, aşa cum este precizat în literatură, provin din domeniul *inteligenței artificiale*, în această lucrare ne vom concentra asupra acestui domeniu, mai precis pe *învățarea automată*. Sunt discutate câteva din tehnicile cele mai importante din acest domeniu şi este arătat cum sunt folosite pentru îmbunătățirea detecției atacurilor. Sunt construite modele sub forma de diagrame UML cu scopul de a arăta şi grafic rolul fiecărei tehnologii în procesul de detecție a intruziunilor. Apoi este prezentat un tabel cu câteva produse comerciale/de cercetare care folosesc algoritmi de inteligență artificială în metodologiile lor de detecție, din articolele din literatură studiate de către autori în realizarea acestei cercetări. La fel ca în orice lucrare de analiză a unui domeniu, cititorului îi sunt oferite referințe din literatură unde poate găsi mai multe informații relevante subiectului discutat.