A SURVEY OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Katanosh Morovat
Department of Mathematics and Computer Science
Western Carolina University
Cullowhee, USA
kmorovat@wcu.edu

Brajendra Panda
Dept. of Computer Science and Computer Engineering
University of Arkansas,
Faytteville, USA
bpanda@uark.edu

Abstract – **During the last decades, not only the number of cyberattacks have increased significantly, they have also become more sophisticated. Hence designing a cyber-resilient approach is of paramount importance. Traditional security methods are not adequate to prevent data breaches in case of cyberattacks. Cybercriminals have learned how to use new techniques and robust tools to hack, attack, and breach data. Fortunately, Artificial Intelligence (AI) technologies have been introduced into cyberspace to construct smart models for defending systems from attacks. Since AI technologies can rapidly evolve to address complex situations, they can be used as fundamental tools in the field of cybersecurity. AI-based techniques can provide efficient and powerful cyber defense tools to recognize malware attacks, network intrusions, phishing and spam emails, and data breaches, to name a few, and to alert security incidents when they occur. In this paper, we review the impact of AI in cybersecurity and summarize existing research in terms of benefits of AI in cybersecurity.**

Keywords–component: cybersecurity, artificial intelligence, machine learning, deep learning, bio-inspired computing, cognitive science

I. INTRODUCTION

The exponential growth of computer networks has led to a tremendous growth in number of cyberattacks. All sectors of our society, from government to economy, to critical infrastructures, are largely dependent on computer networks and information technology solutions. Therefore, they are obviously vulnerable to cyberattacks. A cyberattack is an attack launched from one or more computers against other computers or networks. Typically goal of a cyberattacks is either to disable the target computer, or take the services offline, or get access to the target computer's data [25]. Since the first denial-of-service (DOS) attack in 1988, the number and impact of cyberattacks have been increased remarkably. Indeed, cybersecurity has become one of the most challenging tasks in computer science field; and it is expected that the number and sophistication of cyberattacks will grow continually and exponentially.

Cybersecurity is a technology, process, and practice to protect networks, devices, programs, and data from attacks, damages, or unauthorized accesses. According to the definition provided by Myriam Dunn Cavelty [3], "cybersecurity refers to the set of activities and measures, technical and non-technical, intended to protect the 'real geography' of cyberspace but also devices, software, and the information they contain communicated, from all possible threats". Cybersecurity has become one of the most important issues in cyberspace [4, 5].

Traditional cybersecurity methods work based on response to an attack and rely on the static control of security devices. For instance, in case of network intrusion attacks, security systems monitor nodes according to a pre-defined set of rules. These methods wait to be notified that an attacked has occurred. However, with the increasing number of cyberattacks, the traditional approach is no longer useful. One example of inadequacy of traditional cybersecurity methods is the recent hack of Equifax in 2017, causing a significant risk to sensitive information by exposing data for as many as 143 million customers [9]. Moreover, with the new threat techniques like advanced persistent threats (APTs) and zero-day attacks, attackers typically hide their activities and attacks occur before the software developers discover the vulnerabilities; consequently, it takes a good amount time to fix the vulnerable systems. Evans et al. [7] mentioned about a global shortage of cybersecurity skills. Lack of sufficient cybersecurity skills impact corporations, national security, law enforcement and the intelligent community [8]. During 2014-2015, computer security experts had to respond to a great number of cybercrimes involving Blue Cross / Blue Shield, Anthem, Target, and Home Depot, among others. Attackers hacked government and private computer systems by taking advantage of loopholes and malfunctions in security systems or exploiting the vulnerabilities within the IT infrastructures [10]. So, the traditional passive defense methodologies are no longer sufficient [6]. In today's unpredictable environment, where cyberattacks happen daily and are constantly evolving, the only way for protecting data is using aggressive cyber techniques. Hence, the new approach must prevent attacks from happening in the first place instead of waiting to get notifications after attacks have already occurred.

This research explores the need of evolution of cybersecurity techniques and explains how AI can be utilized to offer optimum solutions for cyber environments and enhance cyber skills against cyber threats. It also

978-1-7281-7624-6/20/$31.00 ©2020 IEEE
DOI 10.1109/CSCI51800.2020.00026

provides an overview of some AI subset technologies such as machine learning, expert system, deep learning, and bio-inspired computations.

The paper is organized as follows: Section II presents a brief overview of AI. Section III introduces AI techniques in cybersecurity. Section IV explains AI-based approaches in cybersecurity. Section V concludes the paper with some suggestions for possible future work, and the final section cites the references.

II. OVERVIEW OF ARTIFICIAL INTELLIGENCE

AI, as a discipline of computer science, has been a popular and ubiquitous concept in the last decade. The term AI was proposed in 1956 by John McCarthy. He described AI as an approach that uses mathematical logic to formalize basic facts about events and their effects [1]. AI, also called machine intelligence, is intelligence presented by machine. It enables programmers to write their programs in a simple way. Complex mathematical algorithms are used in AI to simulate human thinking [11]. AI technologies can understand, learn, and act based on the information derived from events and effects. According to Stuart Russell and Peter Norvig, "AI attempts not just to understand but also to build intelligent entities" and they offered a definition for AI, organized into two main categories, such as [13]:

- thought process and reasoning: these measure success in terms of thinking, which is categorized into thinking humanly and thinking rationally.
- behavior: this measures a success based on the ideal performance and action, and it is categorized into acting humanly and acting rationally.

The following table presents a definition for each category [13].

TABLE I. AI definitions

Thinking Humanly	Thinking Rationally
"[The automation of] activities that we associate with human thinking, activities such as decision-making, problem solving, learning … " (Bellman, 1978)	"The study of the computations that make it possible to perceive, reason, and act." (Winston, 1992)
Acting Humanly	Acting Rationally
"The art of creating machines that perform functions that require intelligence when performed by people." (Kurzweil, 1990)	"Computational Intelligence is the study of the design of intelligence agents." (Poole et al., 1998)

In terms of the above definitions, AI approach focuses on human behaviors, knowledge representations, and methods of inference, and then develops intelligent agents. Agents can interact with other agents and exchange their knowledge. The process of finding a solution to a problem is accomplished based on the knowledge shared among agents, each of which has a decision-making system, which is constructed based on the decision-making theory.

Decision-making theory has two aspects, diagnosis and look-ahead. Jean Pomerol [15] described that AI has many relations with diagnosis, representing and recording human knowledge. Due to uncertainty of look-ahead decisions, AI does not pay enough attention to this aspect and AI disregards multi-attribute human reasoning. Simon [14], offered a bounded rationality model to acknowledge that humans use several criteria at different instants of the decision process, therefore a kind of tradeoff reasoning can be an acceptable solution. So, AI seeks to produce a new type of automate intelligence that responds like human intelligence. To achieve this goal, machines need to learn precisely, which means machines must be trained by learning algorithms. AI methods rely on algorithms. However, even if there is not too much improvement on algorithms, AI can use big data and massive computing to learn through brute force [12].

AI works in three ways [2]:

- *Assisted intelligence*, which improves what people are already doing
- *Augmented intelligence*, which empowers people to do things that they could not do
- *Autonomous intelligence*, which are features of machines that act on their own.

With respect to these three categories, it could be concluded that AI aims to solve some of the most difficult problems and cybersecurity falls into this category, since cyberattacks have become highly sophisticated and potentially more disastrous and turned to be a complex issue in cyberspace.

III. AI TECHNIQUES IN CYBERSECURITY

This section gives a brief overview of the learning algorithms, which are essential concepts of AI, and presents a brief introduction about branches of AI, such as expert system, machine learning, deep learning, and biologically inspired computation that are frequently leveraged in the cybersecurity area.

Learning algorithms are used to train machines as well as increase performance through learning and training from experience. According to the definition given by Mitchel [20], "A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P, if its performance at tasks in T, as measured by P, improves with experience E." Generally, there are three learning algorithms for training machines, as defined below:

- *Supervised learning*: This type has a training process with a large labeled data set. After the training process, the system must be checked with test data set. These learning algorithms are usually used as a classification mechanism or regression mechanism. Regression algorithm generates outputs or prediction values, which are one or more continuous-valued numbers according to the input. Classification algorithms categorize data into classes and in contrast to regression, classification algorithms generate discrete outputs.
- *Unsupervised learning*: In contrast to supervised learning, unsupervised learning uses unlabeled training

data set. Unsupervised learnings are usually used to cluster data, reduce dimensionality, or estimate density.

- *Reinforcement learning*: This type of learning algorithm learns the best actions based on the rewards or punishments. Reinforcement can be considered as a combination of supervised learning and unsupervised learning. Reinforcement learning is useful for situations where data is limited or not given [16].

AI technology contains several subfields some of which are described below.

- *Expert system*(ES): It is also known as knowledge-based system. ES has two main components: the first component is a set of knowledge, which is the core of knowledge-based system and contains accumulated experiences, and the second one is an inference engine, which is used for reasoning about predefined knowledge and finding answers to given problems [18]. According to the reasoning method, expert systems can solve two types of problems, case-based reasoning and rule-based reasoning.
  - Case-based reasoning: This recalls previous similar problem cases, assumes solutions for the past problem case can be used to solve a new problem case. Subsequently, the new solution will be evaluated and might be revised as needed and then added to the knowledge base. This approach continually helps to improve the accuracy of the system and learns new problems gradually.
  - Rule-based reasoning: This uses rules, which are defined by experts to solve problems. Rules consist of two parts: a *condition* and an *action*. Problems are analyzed in two steps: first, the condition is evaluated and then the proper action will be taken. Unlike case-based systems, rule-based systems cannot learn new rules or modify existing rules automatically.

  ESs can be used for decision-making support in cyberspace. In general, modified data of a security system are evaluated and then the security expert system can determine whether a network or system activity is malicious or not. Security experts usually use statistical methods to scan and analyze a large set of modified data in a reasonable time period. Expert systems can successfully support these efforts by performing real-time monitoring in cyber environments. In case of malicious intrusions, security expert systems generate a warning message and relevant information, upon which security professionals could select appropriate security measures [19].
- *Machine learning* (ML): According to the definition given by Arthur Samuel [21], “Machine learning is a set of methods that gives computers the ability to learn without being explicitly programmed.”. ML provides systems the ability to discover and formalize the principles that underlies that data, learn through the data, and improve from experience without being explicitly programmed. The process of learning begins with observing data through examples to look for patterns in data and make a better decision in future based on the given examples. With this knowledge, the algorithm can reason the properties of previously unseen examples [22]. ML uses statistics to extract information, discover patterns, and draws conclusions even while using massive amount of data. There are different types of ML algorithms. In general, they can also be classified into three main categories: *supervised learning*, *unsupervised learning*, and *reinforcement learning*. In the cybersecurity domain, the most commonly used algorithms are: decision tree, support vector machine, Bayesian algorithms, k-nearest neighbor, random forest, association rule algorithms, ensemble learning, k-means clustering, and principle component analysis [17].
- *Deep learning* (DL): This is also known as deep neural learning and uses data to teach computers how to do their tasks that typically humans are capable of doing. DL completely includes ML, where a machine is able to learn by experience and skills without human intervention. Similar to the way humans learn from their experiences, DL algorithms can perform a task repeatedly, each time changing the task a little to improve the outcome. DL imitates the working of human brain in processing data and creating patterns to use in decision making. It adopts the working mechanisms of human brains and neurons of processing signals. By constructing more extensive neural networks and training them with a large amount of data, the performance of neural networks is continuously increased. In many applications, the amount of data generated every day is extremely huge. Because DL algorithms require a huge amount of data to learn from, this increase in daily data creation is one reason that DL is leveraged in cyber environments. One of the advantages of DL over ML is its superior performance in large bulk of data. Similarly to ML methods, DL methods supports supervised learning, unsupervised learning, and reinforcement learning. Typical DL algorithms generally used in cybersecurity domain are: feed forward neural networks, convolutional neural networks, recurrent neural networks, deep belief networks, stacked autoencoders, generative adversarial networks, restricted Boltzmann machines, and ensemble of DL networks [17].
- *Biologically inspired computation*: It is a collection of intelligent algorithms and methods that use biological behaviors and characteristics to solve a wide range of complex problems. Traditional AI and bio-inspired techniques are different due to their learning methods. Traditional AI creates intelligence, which is demonstrated by machine. This intelligence is created by programs, which generate other programs including intelligence. However, bio-inspired computing begins with a set of simple rules and simple organisms, which firmly correspond to those rules. With respect to some conditions, these organisms gradually evolve. Among bio-inspired computations, the following techniques are most commonly used in cybersecurity domain: genetic

algorithm, evolution strategies, ant colony optimization, particle swarm optimization, and artificial immune systems [17].

IV. AI-BASED APPROCHES IN CYBERSECURITY

Our society is changing fast, thanks to advancements in computing technologies, which has had significant impact on people's daily lives and works. Some of these technologies have created machines that can think, learn, decide and solve problems as humans do. AI, as an example, adopts intelligence and can perform real-time analysis and decision making while processing enormous amounts of data to solve problems. Many scientific and technological fields can take advantages of AI methods. It is no secret that, Internet is ripe with a ton of personal information and that causes many cybersecurity issues. First, manual analysis is almost impractical due to the size of data. Second, threats are growing or AI-based threats may happen. In addition, the cost to prevent threats increases because of employing specialists is very expensive. It also takes a lot of time, money, and efforts to design and implement algorithms to recognize those threats. One solution for those issues is to use AI-based methods.

AI can analyze large amount of data efficiently, accurately, and in short time. Using threats history, an AI-based system can know about the past threats and use this knowledge to predict similar attacks in the future, even if their patterns change. AI can be used in cyberspace because of these reasons [17]: AI can discover new and considerable changes in attack, AI can handle big data, and AI security system can learn continuously to respond better to threats.

However, AI has also some limitations, such as: an AI-based system requires a significant amount of data and processing this huge data takes a long time and a lot of resources, frequent false-alarms are an issue for end-users and delaying any required response affects the efficiency. Moreover, attackers can attack the AI-based system by inserting adversarial inputs, data poisoning, and model stealing.

Scientists have recently determined how AI techniques can be leveraged to detect, stop, and respond to cyberattacks. The most common types of cyberattacks can be categorized into four main groups:

- Software exploitation and malware identification
  - Software exploitation: Vulnerabilities exist in software, and a percentage of those are exploitable vulnerabilities, which means an attacker who knows about the flaw can attack the underlying software application. Some popular software vulnerabilities are: buffer overflow, integer overflow, SQL injection, cross site scripting, and cross site request forgery. Some vulnerabilities are discovered and fixed. It would have been ideal, if software developers had found and fixed all vulnerabilities during the design and development process, which is very hard considering software development costs and pressure to release software to market. Hence, finding and fixing problems are done continuously. According to Bruce Schneier, "the internet can be regarded as the most complex machine mankind ever built. We barely understand how it works, let alone how to secure it" [26]. To fix software bugs, going through code line by line is a tedious task, but computers can do that if they are taught what the vulnerabilities look like. It appears that AI has the potential to accomplish these tasks. Benoit Moral [27] described how specifically AI techniques help to improve application security. This research focused on the web application security and advocated the use of knowledge based systems, probabilistic reasoning, and Bayesian algorithms to detect software exploitations.
  - Malware identification: It is a popular method for cyberattacks. Types of malicious software are viruses, worms, and Trojan horses. Since impact of malware on politics and economy is huge, preventing and mitigating attacks caused by malware is vital. So, many researches about adopting AI techniques have been done. Here, some of notable research are listed. The authors in [28] defined a framework for classifying and detecting malware using data mining and ML classification. The scholars in [29] used k-nearest neighbors and support vector machine as ML classifiers to detect unknown malwares. Another approach [30] built a deep learning architecture to detect intelligent malware. A recent research in malware detection focused on mobile malware. In [31], a deep convolutional neural network was adopted to identify malware. In [32], the authors defined a novel ML algorithms, namely, rotation forest, to identify malware. Another research direction was the use of bio-inspired computation for malware classification. This technique was used to optimized parameters to classify parameters. In [33, 34] the authors used genetic algorithms to enhance the effectiveness of a malware detection.
- Network intrusion detection
  - Denial of Service (DoS): This attack, which is one of the most common attacks, occurs when authorized users are unable to access information, devices, or other network resources due to cybercriminals' action. The authors in [41], proposed a system that applies two different approaches, namely, anomaly-based distributed artificial neural networks and signature-based approach.
  - Intrusion Detection System (IDS): An IDS protects a computer system from unusual events, violation, or imminent threats. Due to flexibility, rapid calculations, and quick learning of AI-based technologies, they are appropriate for developing

IDS. The goal of AI-based algorithms is to optimize features and improve classifiers to reduce the false alarm. Authors in [35] combined a support vector machine and a modified version of k-means to create a model for IDS. In [36], the authors presented a fuzziness based reinforcement learning approach for IDS. They used unlabeled sample datasets with a supervised learning to enhance the performance. Another approach, [37], used genetic algorithm and fuzzy logic for network intrusion detection to predict a network's traffic for a given time interval.

- Phishing and spam detection:
  - Phishing attack: A phishing attack attempts to steal user's identification. Brute-force attacks and dictionary attacks are examples of phishing attack. Some notable AI-based approaches to cope with this issue are listed here. The authors in [38] introduced a phishing detection system, called phishing email detection system, which leveraged modified neural network and reinforcement learning. In [39], Feng et al. utilized neural network to identify phishing web sites by adopting Monte Carlo algorithm and risk minimization approach.
  - Spam detection: This refers to uninvited bulk email. Spam emails may have inappropriate contents, which leads to security issues. Recently, AI-based algorithms have been used to filter spam emails. For instance, one system presented by Feng et al. [40]. This system combined support vector machine and naive Bayes algorithm for filtering spam emails.

AI can be utilized in various domains of cyberspace to analyze data for attack detection and response. AI can also automate processes, which helps security analysts to quickly work with semi-automate systems to determine cyberattacks. Some popular approaches to AI in cybersecurity are presented below:

A. Threat detection and classification:
AI methods can identify threats and prevent attacks before they take effect. This is generally accomplished by creating a model of analyzing big datasets of cybersecurity events and recognizing patterns of malicious activities. The model is typically made up of previous data surveillance and recorded Indicators of Compromise (IOC), which are used to monitor, identify, and respond to threats in real time. Consequently, if similar activities are detected, they are automatically recognized using the models. ML classification algorithms uses IOC datasets to identify the different behavior of malwares in datasets and classify them [23]. Furthermore, behavioral-based analysis uses ML clustering and classification algorithms to analyze the behavior of thousands of malwares [24]. It is also possible to use the patterns to automate process of detecting and classifying new threats. In addition, security analysts or other automated systems can get tremendous benefits. For instance, using historic dataset including detailed events of WannaCry ransomware attacks, ML algorithms can learn to identify similar attacks automatically.

B. Network risk scoring:
This is a quantitative measure, which assigns risk scores to different sections of network. This measure is used to prioritize cybersecurity resources based on the risk scores. AI can automate this process by analyzing historic cybersecurity datasets and determine which areas of networks are more vulnerable or involved to certain types of attacks.

C. Automated processes and optimize human analysis:
AI can automate repetitive tasks accomplished by security analysts during security actions. Automating process can be accomplished by analyzing reports on past actions generated by security analysts to identify and respond to certain attacks successfully. AI algorithms use this knowledge to build a model, which can be used later for identifying similar cyber activities. Using this model, AI algorithms respond to attacks without human inference. Sometimes automating the entire security process is difficult. In this case, AI can be incorporated in the cybersecurity work flow, which means system analysts and computers can accomplish tasks together.

V. Conclusions

Rapid growth of cyber threats and sophistication of cyberattacks require new, more robust, flexible, and scalable methods. In current research, the main targets of AI-based algorithms for cybersecurity are malware detection, network intrusion detection, and phishing and spam detection. Various researches leveraged a combination of different AI techniques, such as ML/DL methods together with bio-inspired computation, or different learning methods such as supervised learning together with reinforcement learning. Such combinations yield outstanding results. Although the role of AI in solving cyberspace issues is inevitable, some problems related to trust to AI and AI-based threats and attacks would be another concern in cyber environment.

VI. References

[1] John McCarthy," Artificial Intelligence logic and formalizing common sense," Stanford University, CA, USA 1990

[2] https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/.

[3] Cavelty, Myriam Dunn, " The Routledge Handbook of New Security Studies,". 154-162, 2018.

[4] Guan ZT, Li J, Wu LF, et al., "Achieving efficient and secure data acquisition for cloud-supported Internet of Things in smart grid,". IEEE Internet Things J, 4(6): 1934-1944. https://doi.org/10.1109/JIOT.2017.2690522, 2017.

[5] Wu J, Dong MX, Ota K, et al.,"Big data analysis-based secure cluster management for optimized control plane in software-defined networks,". IEEE Trans Netw Serv Manag, 15(1):27-38. https://doi.org/10.1109/TNSM.2018.2799000.

[6] Jian-hua LI, "Cyber security meets artificial intelligence: a survey,". School of cybersecurity, Shanghai Jiao Tong University, Shanghai, China , 2018.

[7] K. Evans and F. Reeder. "A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters,". CSIS, 2010.

[8] K. Francis and W. Ginsberg, "The Federal Cybersecurity Workforce: Background and Congressional Oversight Issues for the Departments of Defense and Homeland Security".

[9] https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.

[10] McAfee Labs Report, March 2016.

[11] Lidestri, N., Maher, Stephen J., & Zunic, Nev.," The Impact of Artificial Intelligence in Cybersecurity,". ProQuest Dissertations and Theses, 2018.

[12] Anyoha, R., "The History of Artificial Intelligence,". 2019. Retrieved from http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/.

[13] Russell Stuart J., Norvig, Peter *(2003),* " Artificial Intelligence: A Modern Approach, ". (3rd ed.), Upper Saddle River, New Jersey: Prentice Hall, ISBN 0-13-790395-2.

[14] Simon, H.A., "Reason in Human Affairs,", Basil Blackwell, Oxford, 1983.

[15] Jean-CharlesPomerol, "Artificial intelligence and human decision making,". European Journal of Operation Research, March 1997, DOI: 10.1016/S0377-2217(96)00378-5 · Source: CiteSeer.

[16] Arulkumaran K, Deisenroth MP, Brundage M, et al., "Deep reinforcement learning: a brief survey.,". IEEE SignalProcess Mag, 34(6):26-38, 2017. https://doi.org/10.1109/MSP.2017.2743240.

[17] Thanh Cong Truong, Quoc Bao Diep, Ivan Zelinka, "Artificial Intelligence in the Cyber Domain: Offence and Defense,". Symmetry Journal, March 2020.

[18] Nadine Wirkuttis, Hadas Klein, "Artificial Intelligence in Cybersecurity,". Cyber, Intelligence, and Security, Volume 1, No. 1, January 2017.

[19] D. Paul Benjamin, Partha Pal, Franklin Webber, Paul Rubel, Mike Atigetchi, "Using A Cognitive Architecture to Automate Cyberdefense Reasoning,". Proc. Of Conference on Bio-inspired, Learning and Intelligent Systems for Security, August 2008, Edinburgh, UK.

[20] Tom M. Mitchel, "Machine Learning,". McGraw-Hill Science/Engineering/Math; March 1997, ISBN: 0070428077.

[21] Arthur L. Samuel, "Some Studies in Machine Learning Using the Game of Checkers,". IBM Journal, November 1967.

[22] Machine Learning Methods for Malware Detection. Kaspersky Lab, 2020.

[23] Manjeet Rege, Raymond Blanch K. Mbah, "Machine Learning for Cyber Defense and Attacks,". The seventh international conference on data analytics, 2018, ISBN: 978-1-61208-681-1.

[24] K. Rieck, P. Trinius, C. Willems, and T. Holz, "Automated analysis of malware behavior using machine learning,". Journal of Computer Security, 19(4), 639-668, 2011.

[25] Josh Fruhlinger, "What is cyber attack?,". CSO, February 2020. https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html.

[26] Bruce Schneier, "We Have Root,". Wiley 2019. ISBN: 978-1-119-64301-2.

[27] Benoit Morel, "Artificial Intelligence a Key to the Future of Cybersecurity,". In Proceeding of Conference AISec'11, October 2011, Chicago, Illinois, USA.

[28] Chowdhury, M., Rahman, A., Islam, R., "Malware analysis and detection using data mining and machine learning classification,". In Proceedings of the International Conference on Applications and Techniques in Cyber Security and Intelligence, Ningbo, China, 16–18 June 2017; pp. 266-274.

[29] H. Hashemi, A. Azmoodeh, A. Hamzeh, S. Hashemi, "Graph embedding as a new approach for unknown malware detection,". J. Comput. Virol. Hacking Tech. 2017, 13, 153-166.

[30] Y. Ye, L. Chen, S. Hou, W. Hardy, X. Li, "DeepAM: A heterogenous deep learning framework for intelligent malware detection,". Knowledge Information System. 2018, 54, 265-285.

[31] N. McLaughlin, J. Martinez del Rincon, B. Kang, S. Yerima, P. Miller, S. Sezer, Y. Safaei, E. Trickel, Z. Zhao, A. Doupe, "Deep android malware detection,". In Proc of the Seventh ACM on Conference on Data and application Security and Privacy, Scottsdale, AZ, USA, 22-24 March 2017, pp.301-308.

[32] H.J. Zhu, Z.H. You, Z.X. Zhu, W.L. Shi, X. Chen, L. Cheng, "Effective and robust detection of android malware using static analysis along with rotation forest model,". Neurocomputing 2018, 272, 638-646.

[33] F.V. Alejandre, N.C. Cortés, E.A. Anaya, "Feature selection to detect botnets using machine learning algorithms,". In Proceedings of the 2017 International Conference on Electronics, Communications and Computers (CONIELECOMP), Cholula, Mexico, 22–24 February 2017; pp. 1-7

[34] A. Fatima, R. Maurya, M.K. Dutta, R. Burget, J. Masek, "Android Malware Detection Using Genetic Algorithm based Optimized Feature Selection and Machine Learning,". In Proceedings of the 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), Budapest, Hungary, 1–3 July 2019; pp. 220-223.

[35] W.L. Al-Yaseen, Z.A. Othman, M.Z.A. Nazri, “Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system,”. Expert Syst. Appl. 2017, 67, 296-303.

[36] R.A.R. Ashfaq, X.Z. Wang, J.Z. Huang, H. Abbas, Y.L. He, “Fuzziness based semi-supervised learning approach for intrusion detection system,”. Information Science, 2017, 378, 484-497.

[37] A.H. Hamamoto, L.F. Carvalho, L.D.H. Sampaio, T. Abrao, M.L. Proenca, “Network anomaly detection system using genetic algorithm and fuzzy logic,”. Expert System Application. 2018, 92, 390-402.

[38] S. Smadi, N. Aslam, L. Zhang, “Detection of online phishing email using dynamic evolving neural network based on reinforcement learning,”. Decision Support System, 2018, 107, 88-102.

[39] F. Feng, Q. Zhou, Z. Shen, X. Yang, L. Han, J. Wang, “The application of a novel neural network in the detection of phishing websites,” Intelligent Humanizing Computation, 2018, 1-15.

[40] W. Feng, J. Sun, L. Zhang, C. Cao, Q. Yang, “A support vector machine based naive Bayes algorithm for spam filtering,”. In Proceedings of the 2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC), Las Vegas, NV, USA, 9-11 December 2016; pp. 1-8.

[41] Sabah Alzahrani, Liang Hong, “Detection of Distributed Denial of Service (DDoS) attacks Using Artificial Intelligence on Cloud,”. In Proceedings of 2018 IEEE Conference, San Francisco, CA, USA, July 2018.