Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, May : 2023

A NEW PARADIGMS OF ARTIFICIAL INTELLIGENCE AND CYBER SECURITY

[1]Chennaiah Kate, Assistant Professor, IT, St. Peter's Engineering College(A), Telangana, India

[2]Dr. Anjaiah Adepu, Professor, CSE, St. Peter's Engineering College(A), Telangana, India

[3]Sreekanth Kottu, Assistant Professor IT, St. Peter's Engineering College(A), Telangana, India

[4]Chinni Krishnaiah.G. Assistant Professor CSE-AIML,Mallareddy University,Telangana,India

[1]chennaiah@stpetershyd.com , [2]anjaiah@stpetershyd.com,[3]sreekanthkottu@gmail.com

[4]chinnikrishnaiahg@mallareddyuniversity.ac.in

ABSTRACT

The frequency and sophistication of cyberattacks have both greatly grown during the past few decades. Therefore, developing a cyber-resilient strategy is of utmost significance. In the event of a cyberattack, traditional security measures are insufficient to prevent data leaks. Cybercriminals have mastered the use of cutting-edge methods and powerful tools to hack, attack, and compromise data. Thankfully, artificial intelligence (AI) technology has been applied to the creation of intelligent models for securing systems against attackers. AI technologies can quickly advance to meet complicated problems, making them useful as basic cybersecurity tools. Artificial intelligence-based methods can offer effective and potent cyber defense capabilities to identify malware assaults, network intrusions, phishing and spam emails, and data breaches, to mention a few. In this essay, we examine the role of AI in cyber security and analyze the pertinent literature in terms of its advantages.

Keywords: Cybersecurity, AI, ML, deep learning, bio-inspired computing, and cognitive science

INTRODUCTION

The number of cyberattacks has greatly increased as a result of the exponential expansion of computer networks. All facets of modern society, including the government, the business, and crucial infrastructures, rely heavily on computer networks and IT solutions. They are therefore clearly at risk from cyberattacks. An assault launched from one or more computers against other computers or networks is referred to as a cyberattack. Cyberattacks often aim to either cripple the

target computer, shut down the services, or access the data on the target machine [25]. The frequency and severity of cyberattacks have significantly grown since the first denial-of-service (DOS) assault in 1988. In fact, maintaining cybersecurity has grown to be one of the most difficult problems in the world of computer technology, and it is anticipated that both volume and complexity will increase continuously and rapidly. Networks, devices, programmes, and data are protected by networks, processes, and practices known as cyber security from intrusions, damage, and unauthorized access. "Cybersecurity refers to the set of activities and measures, both technical and non-technical, intended to protect the 'real geography' of cyberspace as well as devices, software, and the information they contain communicated, from all possible threats," according to the definition given by Myriam Dunn Cavelty [3]. One of the most crucial challenges in cyberspace nowadays is cybersecurity [4, 5].

Traditional cybersecurity techniques rely on static control of security equipment and operate in reaction to an attack. Security systems, for instance, keep an eye on nodes in the event of network intrusion assaults in accordance with a predetermined set of criteria. These procedures wait until they are informed that an assault has However, the conventional strategy is no longer effective given the rise in cyberattacks.

The recent Equifax attack in 2017 is one instance of how inadequate standard cybersecurity techniques are, putting sensitive information at serious risk by exposing data for up to 143 million clients [9]. Additionally, attackers often conceal their activities with new threat techniques like advanced persistent threats (APTs) and zero-day attacks, and attacks take place before software developers find the vulnerabilities; as a result, it takes some time to fix the vulnerable systems. According to Evans et al. [7], there is a global scarcity of cybersecurity expertise.

Corporations, national security, law enforcement, and the intelligence community are all impacted by a lack of cybersecurity capabilities [8]. Computer security professionals had to respond to a lot of cybercrimes in 2014-2015 involving, among others, Blue Cross/Blue Shield, Anthem, Target, and Home Depot. By taking advantage of security system flaws and malfunctions as well as weaknesses in IT infrastructures, hackers have gained access to both public and private computer systems [10]. Therefore, classic passive defense techniques are no longer enough [6]. The only way to secure data in the uncertain climate of today, when cyberattacks occur often and are continuously changing is by utilizing aggressive cyber methods. As a result, the new strategy must stop assaults from occurring in the first place rather than waiting to get signals after attacks have already taken place.

In order to provide the best solutions for cyber environments and strengthen cybersecurity capabilities against cyber-attacks, this research examines the necessity for the evolution of cybersecurity strategies. Additionally, it gives a brief explanation of a few AI subset technologies, including deep learning, expert systems, machine learning, and bio-inspired computations.

The following is how the paper is set up: A quick review of AI is provided in Section II. Cybersecurity AI approaches are introduced in Section III. The use of AI-based cybersecurity strategies is described in Section IV. The study is concluded in Section V, which also includes some recommendations for potential future research and references.

OVERVIEW OF ARTIFICIAL INTELLIGENCE

In the past ten years, the field of artificial intelligence (AI) has gained popularity and become a common notion. John McCarthy first introduced the term AI in 1956. He defined AI as a technique that formalizes fundamental truths about events and their effects using mathematical reasoning [1]. Artificial intelligence, or AI, is intelligence exhibited by a machine. It makes it possible for programmers to develop their programmes quickly.

AI simulates human thought using sophisticated mathematical algorithms [11]. AI technologies are capable of comprehending, learning from, and acting on data obtained from events and consequences. In their definition of AI, which they divided into two broad categories, Stuart Russell and Peter Norvig stated that "AI attempts not just to understand but also to build intelligent entities" [13]:

- Both mental process and reasoning—which may be divided into the categories of human and rational thinking—measure success in terms of thinking.
- behavior classifies behavior into two categories: acting humanely and acting logically, and it gauges success based on the ideal performance and action.

For each category, a definition is provided in the following table [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	"Computational Intelligence is the study of the design

that require intelligence when performed by people." (Kurzweil, 1990)	of intelligence agents." (Poole et al., 1998)

According to the aforementioned criteria, the AI strategy concentrates on human behaviors, knowledge representations, and inference techniques before creating intelligent agents. Agents can communicate with one another and share knowledge. The process of solving a problem is carried out using the information that is communicated amongst agents, each of whom has a decision-making system that was built using the decision-making theory.

The diagnostic and look-ahead components of decision-making theory are two. According to Jean Pomerol [15], AI has various connections to diagnosing, representing, and storing human knowledge. AI pays insufficient attention to this element and disregards multi-attribute human reasoning since look-ahead judgements are unpredictable. In order to address the fact that people utilise various criteria at various points in the decision-making process, Simon [14] proposed a limited rationality model. As a result, tradeoff reasoning may be a viable option. A new kind of artificial intelligence that reacts like human intellect is what AI aims to create. Machine learning must be accurate in order for this to be accomplished; hence learning methods must be used to train the machines. Algorithms are used in AI techniques. Even if methods are not greatly improved, AI can still learn by brute force using vast data and massive computers [12].

- Assisted intelligence is intelligence that helps individuals accomplish things better already.
- People with enhanced intellect are able to perform tasks they previously could not
- autonomous intelligence, or characteristics of autonomous devices

With regard to these three categories, it can be deduced that AI aims to solve some of the most challenging problems, and cybersecurity fits into this category because cyberattacks have developed into highly sophisticated, potentially catastrophic issues that have become complex.

AI TECHNIQUES IN CYBERSECURITY

In addition to providing a brief introduction to some of the branches of AI that are frequently used in the cybersecurity field, such as expert systems, machine learning, deep learning, and biologically inspired computation, this section provides a brief overview of learning algorithms, which are fundamental AI concepts.

Machines are trained using learning algorithms, which also help them perform better by picking up knowledge and skills through experience. A computer programme is said to learn from

experience E with regard to some class of tasks T and performance measure P, according to Mitchel's definition [20], "if its performance at tasks in T, as measured by P, improves with experience E." For training machines, there are often three learning algorithms, as described below:

- The training method for supervised learning uses a sizable labelled data collection. Following the training phase, the system must be tested using test data. These learning algorithms are often employed as regression or classification mechanisms. According to the input, the regression algorithm produces outputs, also known as prediction values, which can be one or more continuous-valued integers. In contrast to regression, classification algorithms produce discrete outputs after classifying the data into different groups.
- Unsupervised learning: Unlike supervised learning, unsupervised learning makes use of training data sets that are not labelled. Unsupervised learnings are typically applied to data clustering, dimension reduction, or density estimation.
- Reinforcement learning: This kind of algorithm for learning discovers the optimum actions depending on incentives or penalties. A mix of supervised learning and unsupervised learning may be thought of as reinforcement. When data is scarce or nonexistent, reinforcement learning is helpful [16].
- a specialist system (ES) It also goes by the name "knowledge-based system." ES is made up of two main parts: an inference engine used for reasoning about predefined knowledge and determining solutions to problems, and a set of knowledge that serves as the foundation of knowledge-based systems and contains accumulated experience [18]. Expert systems may answer two different kinds of issues using the two sorts of reasoning methods: case-based reasoning and rule-based reasoning.
- Case-based reasoning: This refers to earlier, comparable issue instances and presupposes that the answers to the earlier problem cases may be applied to the current problem case.
- The new answer will then be examined, maybe updated as necessary, and contributed to the knowledge base. This method progressively picks up new issues while helping the system's accuracy increase over time.
- o Rule-based reasoning: This method solves issues by using rules that have been established by experts. Rules have two components: an action and a condition. Problems are examined in two steps: first, the state is assessed, and then the appropriate course of action is chosen. Rule-based systems, in contrast to case-based systems, cannot automatically learn new rules or alter old rules.
- ESs can be applied to help decision-making online. The security expert system may ascertain if a network or system activity is hostile or not after evaluating changed data from a security system. In order to scan and analyze a big set of updated data in a fair amount of time, security specialists typically employ statistical approaches. Expert systems that do real-time monitoring in cyber settings can successfully assist in these endeavors. Security experts can decide on the best security measures by using warning

messages and pertinent information that security expert systems produce in the event of harmful intrusions [19].

- According to Arthur Samuel's definition of machine learning (ML) [21], "Machine learning is a set of techniques that enables computers to learn without being explicitly programmed." With the use of machine learning (ML), systems may learn from data, formalize the underlying ideas, and get better over time without being explicitly coded. In order to find patterns in data and base future decisions on those patterns, the learning process starts with viewing data through examples. The programme may infer the attributes of previously unobserved cases using this information [22]. Even with a vast quantity of data, ML employs statistics to extract information, identify patterns, and make conclusions. Different ML algorithms come in various varieties. They may generally be divided into three groups: reinforcement learning, unsupervised learning, and supervised learning. The most often employed algorithms in the field of cybersecurity are decision trees, support vector machines, Bayesian algorithms, k-nearest neighbor's, random forests, association rule algorithms, ensemble learning, k-means clustering, and principal component analysis [17].
- Deep learning (DL), often referred to as deep neural learning, uses data to train computers how to perform activities that are traditionally performed by people. ML, in which a computer may learn without human intervention via experience and aptitude, is fully included in DL. Similar to how people learn from their experiences, DL algorithms may repeat a job while slightly altering it each time to get better results. DL replicates how the human brain processes information and develops patterns that may be used to decision-making. It uses the signal processing systems seen in human brains and neurons. The performance of neural networks is continually improved by building larger neural networks and training them with a lot of data. The daily amount of data created in many apps is enormous. This rise in everyday data production is one of the reasons that DL is used in cyber settings since DL algorithms need a tonne of data to learn from. The improved performance of DL over ML on huge data sets is one of its benefits. DL approaches allow supervised learning, unsupervised learning, and reinforcement learning similarly to ML methods. Feed forward neural networks, convolutional neural networks, recurrent neural networks, deep belief networks, stacking autoencoders, generative adversarial networks, and limited Boltzmann machines are examples of common deep learning techniques used in cybersecurity.
- Computing that is influenced by biology: This is a group of clever algorithms and techniques that make advantage of biological behavior's and qualities to address a variety of complicated issues. Due to how they learn, traditional AI and bio-inspired systems differ from one another. Machines can build traditional AI, which produces intelligence. These programmes, which also produce other programmes with intelligence, produce this intelligence. However, basic principles and creatures that closely adhere to those laws are the foundation of bio-inspired computing. These creatures progressively develop in response to particular circumstances. The following methods are the ones that are most

frequently employed in the cybersecurity field among bio-inspired computations: Ant colony optimization, genetic algorithms, and evolutionary techniques
Artificial immune systems and particle swarm optimization [17].

CYBERSECURITY APPROACHES BASED ON AI

Thanks to improvements in computing technology, our society is changing quickly. This has a big influence on people's everyday lives and jobs. Machines that can think, learn, make decisions, and solve problems similarly to humans have been made possible by some of these technologies. AI, as an illustration, adopts intelligence and has the capacity to analyze massive volumes of data while performing real-time analysis and decision-making. The use of AI techniques is advantageous in many domains of science and technology. It goes without saying that there is a tonne of personal information on the Internet, which leads to several cybersecurity problems. First, the amount of the data makes manual analysis all but impossible. Second, there may be dangers based on AI or rising threats. Deep learning (DL), often referred to as deep neural learning, uses data to train computers how to perform activities that are traditionally performed by people. ML, in which a computer may learn without human intervention via experience and aptitude, is fully included in DL.

Similar to how people learn from their experiences, DL algorithms may repeat a job while slightly altering it each time to get better results. DL replicates how the human brain processes information and develops patterns that may be used to decision-making. It uses the signal processing systems seen in human brains and neurons.

AI is capable of quickly, correctly, and effectively analyzing massive amounts of data. An AI-based system can anticipate future assaults that will be similar to those that have already occurred by using threat history, even if the patterns of those attacks vary. Because of these capabilities [17], AI may be employed in cyberspace to identify new and significant variations in assault, process large amounts of data, and improve security system response times.

AI does, however, have certain drawbacks. For example, an AI-based system requires a sizeable quantity of data, and processing this volume of data demands a lot of time and resources. Frequent false alarms are also a problem for end users, and delaying any necessary responses reduces efficiency. In addition, attackers can harm the AI-based system by introducing hostile inputs, data tampering, and model theft. Recent research has shown how AI methods may be used to recognize, thwart, and address cyberattacks. Four categories best describe the most prevalent categories of cyberattacks:

- Software exploitation and malware identification
  programme, and some of those flaws can be used to attack the underlying software application by an attacker who is aware of the issue. Buffer overflow, integer overflow, SQL injection, cross-site scripting, and cross-site request forgery are a few common

software vulnerabilities. There are certain flaws that are found and corrected. The ideal situation would have been if software developers had identified and repaired every vulnerability throughout the design and development phase, but this is exceedingly challenging given the high cost of software development and the urgency to get products to market. Therefore, identifying and resolving issues is a constant process.

The internet, in Bruce Schneier's words, "may be considered the most complicated machine mankind has ever made. We hardly even comprehend how it functions, much less how to safeguard it" [26]. Going line by line through the code to correct software defects is a laborious operation, but computers are capable of doing it if they are taught what the vulnerabilities look like. It seems possible that AI might complete these duties. Particularly, Benoit Moral [27] discussed how AI approaches aid in enhancing application security. This study focuses on online application security and recommended using probabilistic reasoning, Bayesian algorithms, and knowledge-based systems to identify software exploitations.

Malware detection is a common technique for cyberattacks. Malicious software can be classified as viruses, worms, and Trojan horses. Malware attacks may have a significant influence on politics and the economy, therefore it's important to stop them and mitigate the damage they inflict. Therefore, there have been several studies regarding implementing AI technology. Here is a list of some noteworthy studies. A methodology for classifying and identifying malware using data mining and ML classification was defined by the authors in [28].

To identify unknown malware, the researchers in [29] employed support vector machines and k-nearest neighbor's as ML classifiers. A deep learning architecture was created using a different method [30] to identify sophisticated malware. The subject of current malware detection study was mobile malware. A deep convolutional neural network was used to detect malware in [31]. To recognize malware, the developers of [32] built a unique ML technique called rotation forest. The use of bio-inspired computing for malware categorization was another area of study. This method was used to optimize parameters for parameter classification. The authors of [33, 34] enhanced the efficiency of malware detection by using genetic algorithms.

- Network intrusion detection

  One of the most frequent assaults is a denial of service (DoS) attack, which takes place when fraudsters prevent authorized users from accessing data, devices, or other network resources. According to the authors of [41], a system that uses both a signature-based method and a distributed artificial neural network based on anomalies is presented.

  IDS: Intrusion Detection System An IDS guards against odd occurrences, violations, and immediate dangers to a computer system. AI-based technologies are suitable for creating IDS because of their adaptability, fast computations, and easy learning. AI-based algorithms seek to decrease false alarms by optimizing features and strengthening classifiers. A support vector machine and a modified version of k-means were used by the authors of [35] to construct a model for IDS. A reinforcement learning strategy for IDS

based on fuzziness was given by the authors in [36]. To improve the performance, they combined supervised learning with unlabeled sample datasets.
Another method, [37], employed fuzzy logic and evolutionary algorithms for network intrusion detection to forecast network traffic for a certain time period.

- Detecting spam and phishing:
  assault through phishing: A phishing assault aims to steal the user's identity. Examples of phishing attempts include dictionary and brute-force assaults.
  Here is a collection of prominent AI-based solutions to this problem. A phishing detection system, referred to as phishing email detection system, was developed by the authors in [38]. It made use of modified neural networks and reinforcement learning. In [39], Feng et al. used a neural network in conjunction with the Monte Carlo method and a risk-minimization strategy to detect phishing websites.
  o Spam detection: Unwanted mass email is what this term refers to.
  Spam emails could include incorrect information, which raises security concerns. Recently, spam emails have been filtered using AI-based algorithms. Consider one system that Feng et al. [40] showed.
  This system integrated naive Bayes with support vector machines.

AI may be used to analyze data for attack detection and retaliation in a variety of cyberspace areas. AI is able to Automate processes to make it easier for security analysts to swiftly identify cyberattacks using semi-automated technologies.

The following list of popular AI cybersecurity methods includes:

A. Threat detection and classification:
   AI techniques can spot dangers and stop assaults before they happen. This is often done by using a model that examines large datasets of cybersecurity events and spots patterns of hostile behavior. Indicators of Compromise (IOC) that have been recorded and previously monitored data are often included in the model, which is used to track, detect, and instantly react to threats.
   As a result, if comparable behavior's are found, the models are used to automatically identify them. IOC datasets are used by ML classification algorithms to identify and categorize the various behavior's of malware in datasets [23]. Additionally, behavioral-based research employs machine learning (ML) clustering and classification algorithms to examine the behavior of hundreds of malwares [24]. The process of identifying and categorizing new threats may also be automated using the patterns. Security analysts and other automated systems can also profit greatly from this. For instance, ML systems may train to recognize such assaults automatically utilizing historical datasets that include specific occurrences of WannaCry ransomware outbreaks.
B. Network risk assessment
   This quantitative measurement provides risk rankings to various network segments. Based on the risk rankings, this method is used to order cybersecurity resources. By

examining historical cybersecurity records, AI can automate this process by identifying the parts of networks that are more exposed to or participating in particular sorts of attacks.

C. Automated processes and optimize human analysis:
AI has the ability to automate routine procedures carried out by security analysts during security operations. Analyzing reports on previous activities produced by security analysts may be used to automate processes and successfully identify and counteract specific assaults. This information is utilized by AI algorithms to create a model that may subsequently be used to find related online actions. With this concept, AI systems react to threats devoid of human interpretation. It might be challenging to fully automate the security procedure. In this scenario, AI may be included into the cybersecurity work flow, allowing system analysts and computers to work together to complete tasks.

CONCLUSIONS

Because of the sophistication of cyberattacks and the rapid increase of cyberthreats, new, stronger, more adaptable, and scalable solutions are needed. According to current research, virus identification, network intrusion detection, and phishing and spam detection are the primary goals of AI-based cybersecurity algorithms. Numerous studies have combined various AI approaches, such as ML/DL techniques with bioinspired computation, or various learning techniques, such as supervised learning and reinforcement learning.

Such mixtures produce excellent outcomes. Even though AI will inevitably play a part in resolving cyberspace challenges, several issues surrounding AI trust and AI-based threats and assaults should still be taken seriously.

REFERENCES

[1] John McCarthy," Artificial Intelligence logic and formalizing common sense," Stanford University, CA, USA 1990
[2] https://www.balbix.com/insights/artificial-intelligencein-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/equifaxcyberattack.html.McAfee Labs Report, March 2016.
[10] Lidestri, N., Maher, Stephen J., & Zunic, Nev.," The Impact of Artificial Intelligence in Cybersecurity,". ProQuest Dissertations and Theses, 2018.
[11] Anyoha, R., "The History of Artificial Intelligence,". 2019. Retrieved from http://sitn.hms.harvard.edu/flash/2017/history-artificialintelligence/.

[12] Russell Stuart J., Norvig, Peter *(2003),* " Artificial Intelligence: A Modern Approach, ". (3rd ed.), Upper Saddle River, New Jersey: Prentice Hall, ISBN 0-13790395-2.
[13] Simon, H.A., "Reason in Human Affairs,", Basil Blackwell, Oxford, 1983.
[14] 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.

[15] 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.
[16] Thanh Cong Truong, Quoc Bao Diep, Ivan Zelinka, "Artificial Intelligence in the Cyber Domain: Offence and Defense,". Symmetry Journal, March 2020.
[17] Nadine Wirkuttis, Hadas Klein, "Artificial Intelligence in Cybersecurity,". Cyber, Intelligence, and Security, Volume 1, No. 1, January 2017.
[18] 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.
[19] Tom M. Mitchel, "Machine Learning,". McGraw-Hill Science/Engineering/Math; March 1997, ISBN: 0070428077.

[20] Arthur L. Samuel, "Some Studies in Machine Learning Using the Game of Checkers,". IBM Journal, November 1967.
[21] Machine Learning Methods for Malware Detection. Kaspersky Lab, 2020.
[22] 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.
[23] K. Rieck, P. Trinius, C. Willems, and T. Holz, "Automated analysis of malware behavior using machine learning,". Journal of Computer Security, 19(4), 639668, 2011.

[24] Josh Fruhlinger, "What is cyber attack?,". CSO, February 2020. https://www.csoonline.com/article/3237324/whatis-a-cyber-attack-recent-examples-showdisturbing-trends.html.
[25] Bruce Schneier, "We Have Root,". Wiley 2019. ISBN: 978-1-119-64301-2.
[26] Benoit Morel, "Artificial Intelligence a Key to the Future of Cybersecurity,". In Proceeding of Conference AISec'11, October 2011, Chicago, Illinois, USA.
[27] 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.
[28] 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.
[29] 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.
[30] 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.
[31] 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.
[32] 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
[33] 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.
[34] W.L. Al-Yaseen, Z.A. Othman, M.Z.A. Nazri, "Multilevel hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system,". Expert Syst. Appl. 2017, 67, 296-303.
[35] 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.