Survey On The Applications Of Artificial Intelligence In Cyber Security

Shidawa Baba Atiku, Achi Unimke Aaron, Goteng Kuwunidi Job, Fatima Shittu, Ismail Zahraddeen Yakubu

Abstract: the rise in cyber attacks has overwhelmed the monetary resources and human ability to analyze and combat every new form of cyber threat in the cyber security industry. With the increasing digital presence, there is a large amount of personal and financial information that should be protected from cyber attacks. In fact, cyber attacks can ruin the reputation of an organization or letdown the organization completely. This research examines the use of AI in the enhancement of cyber security. Recent developments in artificial intelligence are transformational and have exceeded the level of human performance in tasks such as data analytics. The study adopted the thematic literature review method, and data were sourced from Google scholar, science direct, research gates, academia, and others. The investigation revealed that application of AI in controlling cyber attack has advantages and disadvantages; however, the advantages outweigh the disadvantages. This researcher discovers that with the speedy and efficient technology required to operate AI systems, they are likely to improve the protection of customers and businesses in the cyberspace. This is proven by the increasing deployment of AI engines rather than conventional scanning engines in cyber security.

Index Terms: Artificial Intelligence (AI), AI Engines, Cyber Attacks, Cyber Security, Deep Learning (DL), Machine Learning (ML), Scanning Engine

1. INTRODUCTION

Cyber security is concerned with devising shield methods that safeguard computing infrastructures, networks, applications and data against illegitimate access, modification or vandalism [5]. It also involves a collection of methods applied to safe guard the integrity of system networks, applications, and stored information against damage, illegitimate access and assault by cyberpunk [12]. As information and communication technology (ICT) advances, new threats are emerging and changing rapidly. AI, which concerns the science and engineering of making machines intelligent [13], has continued to grow significantly, and it is influencing all aspects of business and life [5]. AI is bringing gains to areas like gaming, manufacturing, health industries, education, natural language processing, and many more. These gains are experienced in cyber security as AI is used for both attack and defense in the cyberspace. The fields of cyber security and AI, which were thought of as separate fields, are increasingly being developed to relate in areas like programs creation which attempts to fix data leakage and improve systems security as attackers focus on mimicking the legitimate processing at human client level among others [1].

Cyber-attacks are growing in amount and complexity; however, what is more worrisome to companies and organizations is their lack of readiness especially from business perspective [2]. It is estimated that the solutions employed at the endpoint like advanced heuristics and signature based can provide 85% - 95% protections against cyber attack [3]. Cybercrime has transited from what was mostly seen as digital scribbles designed to cause mayhem in the past to a multibillion dollar universal industry focusing on peak ranked brands, governments, monetary institutions, and individuals. Latest research shows that malicious software writers see about 1,425% return on investment (ROI) [3]. With such a profitable trade, it is no shock that these perpetrators will consistently explore novel techniques to compromise systems; hence, pressure the cyber security industry to unfold rapidly to forecast and contravene novel threats. The scope of cyber security and AI usage continues to expand largely due to the proliferation of the internet. Hackers get smarter and innovative in creating malicious software to exploit individuals, organizations and governments. These attacks can be in the form of phishing, passwords attacks, virus attacks etc. where conventional security methods may be inadequate. The introduction of AI tends to promote cyber security [4]. AI systems can help, not only in threats detection, but also in taking proactive actions against cyber attacks like to sort and categorize events and threats which eventually relief technicians from repetitive tasks [6]. This investigation captures a brief background of AI in the field of cyber security and its application in cyber security, with narrative literature reviews on the different threats handled by different AI methods. The subsequent sections of this paper are arranged as follows: Section 2 presents the research methodology used at the conduct of the study. Section 3 presents the recent trends of AI in cyber security. Section 4 highlights some AI methods used for cyber security. Section 5 provides some of the benefits and challenges of AI application in the field of cyber security. In Section 6, the discussion of the study is presented. Section 7 presents new perspective for future research. Finally section 8 is the conclusion.

- *Corresponding Author: Ismail Zahraddeen Yakubu, Federal Polytechnic, Bauchi, Bauchi Nigeria, ysbfamily2010@gmail.com*
- *Shidawa Baba Atiku, Directorate of Research, National Institute for Policy and Strategic Studies, Kuru, Nigeria atikushidawa@gmail.com*
- *Achi Unimke Aaron, Computer Science Department, University of Nigeria, Nsukka, aaron.achi.pg02692@unn.edu.ng*
- *Goteng Kuwunidi Job, Computer Science Department, Bogoro College of Education, Bogoro, Bauchi State, kunygoteng@gmail.com*
- *Fatima Shittu, Department of Computer Science, Federal Polytechnic Damaturu, fsbinta1234@gmail.com*

2. RESEARCH METHODOLOGY

This study adopted the thematic literature review methodology. The literature search was guided by using keywords and keywords mix related to the topic to retrieve relevant materials from the following databases: Google scholar, Science Direct, Research Gates and Academia. Secondly, only related literatures published within the last five years were considered because this paper aims to present an overview of recent developments of Artificial Intelligence applications in the area of cyber security. Manuscripts published later than five years but had novel approaches were selected. Manuscripts with more than five citations were selected also. The following sets of materials were ruled out:

papers with subject title not within the scope of this study, papers not written in English, books and patent documents. We scrutinize the abstract as well as the conclusion sections of the consulted materials for pertinent information. According to this step, a confirmation check was done from classified papers against the key phrase in the topic of the paper which is AI application in cyber security. Thus, papers adjudged most relevant to this study were selected.

3. AI IN CYBER SECURITY

The concept of AI was proposed in the year 1956 by John McCarthy as the science and engineering of producing intelligent automata, particularly intelligent computer applications. It is concerned with how to make computers think, work, learn and behave intelligently like humans [5]. The application of AI now affects several aspects of human experience such as expert systems, computer vision, pattern recognition, speech recognition, language translation, robotics, biometric systems, and internet of things (IoT) among others [12]. Despite the wide application of AI, human inference is still needed for monitoring its activities, largely because it can also be used for destruction [12]. Cybercrime is now more common, and it threatens the progress of governments, banks, and multinational companies on a daily basis through online hacking. AI systems adopt techniques that can help overcome short comings of traditional cyber security tools through their flexibility and adaptability [7]. Though AI is already improving cyber security [8], but there are some critical considerations. Some consider artificial intelligence as an emergent threat to humanity [9]. This has raised the concerns of scientists and legal experts about the growing role self-contained AI applications play in cyberspace and their ethical justifiability [10]. AI-systems can be altered, bypassed, and fooled to generate security issues for applications like network monitoring systems, monetary systems, as well as self controlled vehicles. Hence, Safe and resilient methods and robust practices are crucial. In cyber security, Artificial Intelligence has being applied so far to promote defenses. According to its strong automation and data analysis potentiality, AI can be employed to examine huge volume of data efficiently, accurately, and speedily. An Artificial Intelligence system detects analogous attacks that occur in future based on its knowledge and understanding from past threats, even if the mode of attacks changes [5]. Furthermore, AI systems can ascertain novel and complex modifications in attack changeability, contend huge amount of data effectively, and learn to identify threat according to applications' behavior and the entire network activities among other several advantages [5]. AI practices do well in interference detection, and they facilitate response to anonymous threats as they are expected to learn and adapt to conditions, and are proficient in identifying even the tiniest changes in network settings; hence they have the potential to be more prompt than humans when it comes to analyzing unusual types of cyber-attacks.

4. AI METHODS USED FOR CYBER SECURITY

A huge number of methods were introduced in the field of Artificial Intelligence to address issues that need intelligence from human perspective. Some of these methods have developed and accurate steps based on the existing methods. These methods are broadly known in application areas such as data mining which surfaced from subfield of Artificial Intelligence. An overview of this sort may not present a full study of all practically useful Artificial Intelligence techniques; instead, the methods and architectures have been grouped into several divisions: machine learning, neural networks, intelligent agents, data mining and constraint solving, expert systems, search. We describe these divisions and provide references to the applications of individual approach in cyber security.

4.1 Artificial Neural Networks (ANN)

ANN is a statistical learning model mimicking the structural and functional behavior of the human brain, first created as a perception in 1957 by Frank Rosenblatt. ANN has the ability to learn and solve problems in different complex domains. It can learn from data in any domain and address absorbing concerns by merging with disparate nerves. In cyber security, ANNs have been used within all four stages of integrated security approach (a holistic categorization of cyber defense framework), consisting of early warning phase, prevention phase, detection phase and reactive/response phase [14]. ANN can be used to monitor traffic flow in computer networks when integrated in cyber security, thereby detecting malicious intrusions before an actual attack [15] and hindering cyber attacks eventually through perimeter defense [16]. ANN can learn from previous network activities and assaults so as to avoid later attacks. When deep learning (DL) - an advanced form of ANN- is applied to cyber security, the system can recognize suspicious as well as legal files with no human intervention. This method produce better outcome in identifying threats than the conventional methods applied in cyber defense. The general form of an ANN is depicted in fig 1 below.

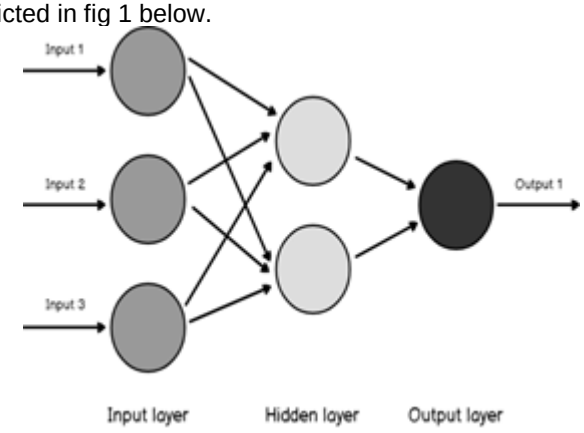

Fig. 1. Artificial Neural Network

ANN's main advantages are its capability to identify patterns in highly non-linear problems and its high speed classification time [18] unlike manual methods used by security experts with experience. Artificial Neural Networks are capable of detecting normal and abnormal network patterns automatically by using previously transferred data over the network. ANNs are employed by network security tools like Firewalls, network hubs and intrusion detection systems to scan network traffic. Deep neural network (DNN) or deep learning, which is a more advanced form of ANN with high computation cost [19], has shown greater advantages as it does not only protect against cyber attacks, but it also predicts the occurrence of these attacks. Hardware improvements have resulted to progressions in data

processing among network resources and improved storage capacities; hence, making DNN more suitable. New developments in DNN technology, such as spiking neural networks that emulate living neurons, provide high application chances; for example, the usage of field programmable gate arrays (FPGAs) allows quick development of neural networks and their adjustments to change threats [16]. A study demonstrated [20] where a committed Artificial Intelligence based security program employ DNN methods to predict cyber attacks, and it showed 85 percent success rate. This success recorded in DNN is opening up new phase of cyber security known as cyber attack prediction. The conventional DL algorithms often used in the field of cyber security [5] includes: generative adversarial networks (GAN), feed forward neural networks (FNN), deep belief networks (DBN), convolution neural networks (CNN), restricted Boltzmann machines (RBM), stacked autoencoder's (SAE), recurrent neural networks (RNN), and ensemble of DL networks (EDLN).

4.2 Security Expert Systems

Expert systems are computer software's developed to enable decision support for sophisticated problems within a specific domain. It consists of a knowledge base which holds knowledge related to the domain under consideration and an inference engine for reasoning and finding answers to given problems [16]. Application areas of expert systems include medical diagnosis, finances or cyberspace. Expert systems vary greatly from small to large technical diagnostic systems and complex hybrid systems in addressing sophisticated issues. Theoretically, an expert system consists of a knowledge base where the knowledge about the domain under consideration is stored and an inference engine for obtaining response from the knowledge base, and probably, added knowledge concerning the situation. Expert systems are used in different problems classes guided by the way reasoning is done. In a case-based reasoning (CBR) approach, problem solving is done by recollecting prior like cases; then a solution is provided by adapting the past solution to a new problem case. The new solutions are then evaluated and revised where needed, thereby improving the accuracy and learning ability of the system. Rule-based systems (RBS) solve problems by applying rules defined by experts. Rules consist of the condition part and the action. Problems are analyzed by first evaluating the condition part; then the action to be taken is determined. Security expert system follows a set of guidelines to combat cyber attacks. It checks the process against the knowledge base; if it is a good and known process then the security system considers it safe; otherwise, the system would flag it as a threat or harmful, and then terminate the process. If there is no such process in knowledge base, then, the system determines the state of the machine by applying the sets of rules in inference engine. The machine state can be severe, moderate or safe. According to the state of the machine, the system notifies the manager or the user regarding the status, and then the inference as detected by the knowledge base.

4.3 Intelligent Agents

Intelligent agent (IA) is a self controlled entity with separate internal decision-making mechanism and a personal objective. It observes via sensors and monitors the domain using actuators and controls its actions towards the achievement of the objectives. Intelligent agents may also learn or use information to achieve their objectives [17]. They may have responsive characteristics, and when communicating with other autonomous agents they may understand and respond to changes in their domain. This enables them to adopt themselves as they attain experience over time [21] through learning and communicating with their environment. IA is created to avoid Distributed Denial of Service (DDoS) attacks. A potent way to use agents against distributed cyber attacks is through construction of artificial "Digital police" which should consist of mobile intelligent agents; hence, requiring implementation of infrastructure to support mobility and communication of cyber agents [16].

4.4 Search

Search is a pervasive approach for critical thinking which may be linked to a wide array of situations in the absence of alternate approach for critical thinking to be applied. It is an everyday problem-solving strategy applied subconsciously by individuals. When applying the search strategy, little knowledge about it is required before a general search algorithm in its formal setting is performed. Some form of search algorithm is built into almost every intelligent program, and its efficiency greatly impacts the performance of the whole program. A wide variety of search methods were developed which takes into account the specific information relevant to issues of inquiry. Although various search methods were developed in AI such as the αβ-search estimation which is employed as a part of various projects, they are rarely used in AI. The αβ-search estimation was originally developed for PC chess. It adopts the "isolate and vanquish" strategy in critical thinking, and it is specifically useful in primitive leadership when two foes are picking their most ideal activities [1].

4.5 Bio-Inspired Computation Methods

Bio-inspired computing is a sub-field of Artificial Intelligence more studied in recent times. It consists of smart algorithms and techniques that mimic the bio-inspired behaviors and attributes to address a broad range of sophisticated academic, as well as real environment problems. Techniques like Ant Colony Optimization (ACO), Evolution Strategies (ES), Artificial Immune System (AIS), Particle Swamp Optimization (PSO), and Genetic Algorithms (GA) are biologically inspired techniques commonly employed in the field of cyber security. The application of bio-inspired techniques in the classification of computer malwares is gaining more acceptances among scientists. These techniques were primarily applied to optimize features and parameters for the classifiers. For instance, PSO was employed in [23] and GA in [24] to improve the efficiency of malware detection system. Again, in a study [25], GA and fuzzy logic was used for intrusion detection. A digital signature of a network segment using glow analysis was created using the GA to predict traffic behavior of a network for a specific time period. In addition, the fuzzy logic method was employed to determine the anomaly or otherwise of an instance on the network. Network traffic from a university was used to conduct the evaluation, 96.53% accuracy and 0.56% false notification were obtained.

5 BENEFITS AND CHALLENGES OF AI APPLICATION IN CYBER SECURITY

The numerous gains and application areas of AI in cyber security have undoubtedly come with some challenges. These challenges can be referred to as the dark side of AI for cyber security. Some of the benefits are discussed below

5.1 Benefits of AI in Cyber Security

A review [26] on the advantages of Artificial Intelligence in the field of cyber security reveals that institutions that implemented AI in cyber security realize significant benefits. This is evident as ROI of two out of three organizations increased on cyber security tools. For example, Siemens AG, leader of Global electrification, automation, and digitalization used Amazon Web Services (AWS) to create AI based, high-speed, self-controlled, and extremely elastic platform for its Siemens Cyber Defense Center (CDC). The AI deployed was able to estimate 60,000 potential assaults per unit time. As a result of the AI deployed, this capability was managed with a team consisting of less than dozen members without any negative impact on system performance. Employing AI in cyber security permit institutions to comprehend and reapply prior threat patterns in identification of novel threats [26]. This results to preservation of time and effort in identifying and investigating incidents, and remediate threats. About 64% of administrators reveal that AI cut down the cost to identify and react to breaches. Fast response is essential in evading cyber attacks. Cost reduction for organizations is within an average of 12%. AI offers opportunities for cyber security largely because the cyber security landscape is rapidly moving from identification, manual response and mitigation towards automated mitigation. AI can identify novel and complex modifications in attack extensibility. Conventional technology focuses on proven intruder and intrusion; and it permit blind spots when identifying unusual activities in novel intrusion. The drawbacks of the early security technology were resolved via smart technology. For instance, activities of the privileged intranet can be watched, and any expressive changes in privileged access operations may represent a potential threat. Predictive Artificial Intelligence offer the security teams an edge required to prevent threats before they cause any mishap. In the UK, Dark trace employs machine learning techniques to mark patterns and detect potential cyber crime in various sectors like manufacturing industries, retails and energy and transportation firm. This is functional as cyber attacks are getting more complex and intruders are developing novel tactics. AI has the ability to handle huge volume of data, improve network security through building of self controlled security systems to identify various attacks and react to breaches. The number of daily security alerts may highly overturn the security groups. Automatic detection and response to intrusion has reduced the efforts required by security experts, and it can be more effective in identifying threats than other techniques. When huge volume of security data is generated and transferred over the network on daily basis, it becomes very difficult to rapidly and reliably track and identify them by the network security experts. Therefore, Artificial Intelligence may assist to expand the monitoring and identification of dubious activities. This can assist network security experts to respond to novel situations; thereby substituting the time consuming manual method of analysis. AI security systems are capable of learning, with time, to react better to attacks: AI assists in identification of attacks according to application characteristics and the entire network's activity. Over time, AI security system understands the regular traffic behavior, and set a threshold for normal activities. Therefore, any deviations from the norm can be termed an attack.

5.2 Challenges of AI Application in Cyber Security

Large number of input samples is required to build an Artificial Intelligence system. It is highly time consuming to obtain and process the samples and require lot of resources. Large number of resources such as memory, processing power and data are required to build and maintain the fundamental system. Skilful resources essential to execute this technology are costly. Frequent false alarm is a challenge for end client. It disrupts businesses by procrastinating essential responses which entirely affects the business efficiency. The process of fine-tuning is a trade-off between minimizing false alarms and sustaining the level of security. Various techniques like adversarial inputs, model theft and data poisoning maybe used by Attackers to target the AI system. Integrated AI systems consist of four main elements: perception, learning, decisions and actions. These systems run in sophisticated environment that needs the elements to interact and be mutually dependent (e.g. misperception may lead to inconsistent decision). Furthermore, each element has a peculiar vulnerability (e.g. perception is liable to training attacks while decisions are exposed to classic cyber exploits) [11]. Lastly, the idea of consistency is not a purely logical matter: additives and lack of certainty need bounds for every element to prevent the system from misbehaving. A formal method is required to independently verify the logical correctness, decision theory and risk analysis of both AI and ML elements. Novel techniques are required to define the system expectations and how to reacts to attacks. Artificial intelligence in cyber security generates a novel threat to digital security. The ability for AI technology to consistently detect and prevent cyber attacks has made attackers to launch more complex attacks. This is, in part, because the cost of developing and adopting the technology reduces as the access to improved AI solutions and ML tools increases. This shows that more sophisticated and adaptive vicious programs can be developed at lesser cost to illegitimate users. These factors have resulted to increase in the task of cybercrime control. One of the less-acknowledged risks of artificial intelligence in cyber security concerns the human element of complacency. Employees may be less conscious of prevention, when an institution adopts AI and ML strategy in its cyber security. We do not need to make emphasis on the high risk of complacent and uninformed employees as the significance of cyber security awareness was already discussed.

6 DISCUSSIONS

This study reports an overview of AI application in cyber security. The use of Artificial Intelligence in cyber security is opening up new borders of investigations in the security landscape. AI is continually proving to be the most effective tool against cyber threats especially in terms of complexity and number. From the literatures reviewed, it is clear that Artificial Intelligence based methods can be employed in the

cyber domain where a diverse methods currently in use are proven ineffective. Research's are conducted in the area of AI application in cyber security and published yearly. Figure 2 below shows the publications of the research output in the domain which this study covers within the time frame mentioned in the methodology section which is 2.0. Figure 2 also shows the trend of papers published on the application of AI in the field of cyber security, especially in recent times. The chart in figure 2 shows that researchers are dwelling on AI application in cyber security and the trend is expected to grow faster in future as the cumulative frequency of publications after 2015 outpaced publications before 2015 in the research domain been considered in this paper.

Fig. 2*. Distribution of literatures by year of publication*

Figure 3 shows the distribution of sourced literatures in the domain of enquiry covered in this work by the databases searched. As earlier mentioned in section 2.0 above, the literatures used in this work were sourced from the following databases: googlescholar, sciencedirect, research gates and academia.

Fig 3*: Distribution of Literatures by database search*

7 NEW PERSPECTIVES FOR FURTHER RESEARCH

The findings on the degree of vulnerability of AI elements to adversarial actions have raised a lot of concerns about the security of data processing environments. AI elements disregard the conventional software analysis and introduced novel attack vectors in AI algorithms operational environments. As a result of hidden dependencies, many applications may be affected. A lot of researches are required to develop theories, engineering principles and practices when employing Artificial Intelligence as system element. This [11] should include modeling of threats, safety tools, environment vulnerabilities, and preventing human machine collaboration. These models should be designed based on AI expertise and should abstract and refine attacks iteratively. Also, it should take into account of data availability, data integrity, data access control, network operation, privacy and a dynamic policy environment.

8 CONCLUSIONS

Advances in ICT have resulted to the emergence of novel challenges for cyber security. Security threats have become so complex such that traditional techniques based on inferences from prior attacks don't seem to help anymore. The computational complexity of cyber attacks requires novel techniques that are more ideal, scalable, and elastic. This paper presents an overview of AI application in cyber security. Some AI methods applied in cyber security were discussed such as DL or DNN, security expert systems, search and some bio-inspired techniques for cyber security. Some areas where AI is impacting on cyber security are malware prediction and detection; intrusion prediction detection and prevention; protection against DDoS, where digital police are employed; and many others. Some benefits and challenges of AI application in cyber security were also discussed. The benefit ranges from speed and accuracy in handling large volumes of data, which is humanly impossible to handle; overall reduction in the cost of securing organizations' valuable data and resources; and increased ROI on AI powered cyber security tools amongst others. The challenges of AI applications for cyber security include the risk of adversarial AI attacks and complacency of the human factor. Despite the drawbacks of the increase in the application of AI in cyber security, it is still believed that its benefits outweigh the challenges. The human element is still integral to cyber security. This is why more industry experts are arguing that AI should be integrated into the systems within each business's cyber security operation center.

REFERENCES

[1] S. Bhutada and P. Bhutada, Application of Artificial Intelligence in Cyber Security: in IJERCSE, 2018, 5(4): 214-219

[2] P.V. Alberto, lecture, Topic: Application of Artificial Intelligence (AI) to Network Security", ITEC 625, University of Maryland, University College, Maryland, Mar. 2018.

[3] Avira, The Application of AI to Cybersecurity – An Avira White Paper, Germany, Avira Operation, 2017.

[4] S. A Panimalar, U.G. Pai and K.S. Khan, "AI Techniques for Cyber Security", International Research Journal of Engineering and Technology, vol. 5, 3, pp. 122-124, Mar. 2018. Available: https://www.irjet.net [assessed May. 29, 2020]

[5] T.S. Tuang. Diep.Q. B, and Zelinka. I, Artificial Intelligence in the Cyber Domain: Offense and Defense: Symmetry, 2020, 12,410 available: www.mdp.com/journal/symmetry on [assessed Apr. 20, 2020]

[6] E. Kanal, Machine Learning in Cybersecurity: Carnegie Mellon University Software Engineering Institute, available onhttp://insights.sei.cnu.edu./sei_blog/2017/06/machine_learning_in_cybersecurity.html

[7] D. Selma, C. Huseyin and A. Mustafa, Application of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review, International Journal of Artificial Intelligence &Applications, vol. 6, issue 1, pp. 21-39, January 2015.

[8] T. Enn, “Artificial Intelligence in Cyber Defense”, in Proceedings of 3rd International Conference on Cyber Conflicts [ICCC], 7-10 June, 2011 Tallin Estonia.
[9] P. Dennis, A. Stuart, “Global Challenges: Twelve risks that threaten human civilization, Global Challenges Foundation”: 2015,Available: http://globalchallenges.org /wp-content/ uploads/12-Risks-with-infinite-impact.pdf [accessed Jun. 3, 2020]
[10] R. Stuart, D. Daniel, T. Max, ‘‘Research Priorities for Robust and Beneficial Artificial Intelligence’’, AI Magazine, vol. 36, issue 4, pp. 105-114, Winter 2015
[11] National Science & Technology Council, “Artificial Intelligence and Cybersecurity: Opportunities and Challenges” Net. & Info.Tech R&D Sub-comtt and the ML & AI Sub-comtt, 2020.
[12] A. M. Shamiulla, Role of Artificial Intelligence in Cyber Security, International Journal of Innovative Technology and Exploring Engineering, vol. 9 issue 1 pp. 4628-4630, November 2019
[13] P. Pranav, “Artificial Intelligence in cyber security”, International Journal of Research in Computer Applications & Robotics, vol 4, 1, pp.1-5, May 2016
[14] J. Kivimaa, A. Ojamaa, E. Tyugu. Graded Security Expert System. Lecture Notes in Computer Science, v. 5508. Springer, 2009, 279-286.
[15] B. Christain, D.A. Elizondo and T. Watson, “Application of artificial neural networks and related techniques to intrusion detection”, World Congress on Computation Intelligence, pp 949-954, 2010
[16] E. Tyugu, “Artificial Intelligence in Cyber Defense”, International conference on Cyber Conflict, vol. 3, pp. 95-105, Tallinn, Estonia, Jan. 2011
[17] W. Nadine and K. Hadas, “Artificial Intelligence in Cybersecurity”, Cyber, Intelligence, and Security, vol. 1, 1, pp. 103-119, Jan. 2017
[18] S. Dima, M. Robert, B. Zvi, S. Shahar and E. Yuval, “Using Artificial Neural Network to Detect Unknown Computer Worms”, Neural Computing and Applications, vol.18, 7, pp. 663-674, Oct. 2009
[19] E. H. Geoffrey, O. Simon and T. Yee-Whye, “A Fast Learning Algorithm for Deep Belief Nets”, Neural Computation, vol. 18, no. 7, pp. 1527-1554, 2006
[20] V. Thomson, “Cyber Attacks Could be Predicted with Artificial Intelligence”, iTechPost,www.itechpost.com/articles/1734 7/cyber-attacks-predicted-artificial-intelligen ce-help.htm, Apr. 21, 2016 [Jun. 2, 2020]
[21] S. Franklin and A. Graesser, “Is It an Agent, or Just a Program? A Taxonomy for Autonomous Agents”, Third International Workshop on Agent Theories, Architectures, and Languages, no. 3, pp. 21-35, 1997
[22] Y. Xia and L. Junshan, “A Security Architecture Based on Immune Agents for MANET”, International Conference on Wireless Communication and Sensor Computing, no. , pp. 1-5, 2010
[23] M. F. AbRazak, etal, “Bio-inspired for features optimization and malware detection.Arabian Journal of Science and Engineering, no. 43, pp. 6963–6979. 2018
[24] A. Fatima, etal, “Android Malware Detection Using Genetic Algorithm based Optimized Feature Selection and Machine Learning”, In Proceedings of the 42nd International Conference on Telecommunications and Signal Processing (TSP), Budapest, Hungary, 1–3 July 2019; pp. 220–223.
[25] R.A.R Ashfaq, etal, “Fuzziness based semi-supervised learning approach for intrusion detection system”. Inf. Sci. 2017, 378, 484–497.
[26] L. Lazic, “Benefits from AI in Cyber Security”, The 11th international Conference on Business Information Security, 18th Oct. 2019, Belgrade, Serbia, pp. 1-9