EAI Endorsed Transactions
on Creative Technologies

Review Article **EAI.EU**

An overview of the applications of Artificial Intelligence in Cybersecurity

Muhammad Shoaib Akhtar, Tao Feng*

School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China

Abstract

The rates at which cyber-attacks are performed have made the cybersecurity unprotected and make it impossible for the security experts to evaluate and combat every new type of cyber-attack. Today's digital age necessarily requires the protection of a vast amount of valuable electronic data from cyber-attacks. Cyber-attacks can destroy the reputation of organizations even shutdown organizations. The protection of cybersecurity is inevitable. In this paper, we have highlighted the potential applications of AI in cybersecurity. Artificial intelligence has advanced to the point where it has surpassed human performance in tasks like data analytics. This study was carried out using systematic literature review; the relevant literature was collected from google scholar, research gate, science direct, IEEE Xplore, Digital Library and Microsoft academic search engines and databases. Our study resulted that AI applications in cybersecurity have many advantages than disadvantages. AI-based applications of cybersecurity can improve the security of cyberspace. This is evidenced by the rising of AI engines in computer security rather than traditional scanning engines.

Keywords: Artificial Intelligence (AI), Cyber-attack, Deep learning, Cybersecurity, Intrusion Detection, Machine learning

Received on 30 September 2021, accepted on 22 November 2021, published on 23 November 2021

doi: 10.4108/eai.23-11-2021.172218

1. Introduction

Cybersecurity is a safeguard that provide protection to computer systems, networks, and electronic data from information disclosure, theft, illegitimate access, as well as from service disruption (Schatz et al., 2017; Atiku et al., 2020). There are various definitions of cybersecurity proposed by different researchers. Sarker et al., (2021) presented a general definition of cybersecurity considering all the valid definitions. According to Sarker et al., (2021), cybersecurity deals with security of anything in cyber world (i.e., information security, network security, operational security, application security, Internet of Things (IOT) security, cloud security and infrastructure security). Cybersecurity is characterized by the collection of methods that encompasses everything involved in the protection of sensitive, personal, governmental, industrial, and other electronic information from cyber criminals, assaults, and adversaries (Srivastava et al., 2021). From 2016 to 2021, investment on worldwide cybersecurity is expected to increase more than $1 trillion (Morgan, 2019).

Internet usage is become essential in the daily routine of modern generation. The amount of data we exchanged on daily basis is huge and enormous. On the hand the number of cyber-attacks is also increasing at a dramatic rate. Every few months, cybercriminals double the potency of their tailored attacks for half the price (Stevens, 2018). Moreover, as cyber-attacks become more sophisticated and automated, cybersecurity becomes ineffective (Truong et al., 2020). According to published literature, traditional approaches of cybersecurity (e.g., network protection systems and computer security systems) proved ineffective against the continuously evolving, transformational and creative attempts of cyber-attacks (Kabbas et al., 2020, Truong et al., 2020). Therefore, we need to find a way to combat newly developing cyber threats and malwares. Here, artificial intelligence (AI) is one of the approaches which can be

*Corresponding author. Email: 13.cs.194@gmail.com used effectively in cybersecurity (Soni, 2020). Machine learning (ML) and deep learning (DL), two recently developed fields of AI, have proved much effective in fighting cyberattacks (Zeadally et al., 2020).

The idea of AI was presented by John McCarthy (1956), AI is the science and engineering of producing intelligent automatic security systems. The main purpose of AI is to trained computers to think, learn, work, perform and behave intelligently and intellectually like human beings (Tuang et al., 2020). AI in this digital age providing services in several areas including computer vision, pattern recognition, expert systems, language processing and translation, speech recognition, biometric systems, robotics, and Internet of Things (IoT) and other related things (Shamiulla, 2019). AI is a major branch of computer science it deals with the systems which are intellectual and independent like human brain (Helm et al., 2020).

In the digital age, cybersecurity is a hot topic, and the role of AI in cybersecurity is more important than ever. When artificial intelligence was first proposed, it was quickly adopted in a variety of fields, including natural language processing, gaming, healthcare, manufacturing, and education (Zeadally et al., 2020). AI possess powerful data analytics capabilities and it can be used to study huge and large amounts of electronic data with great speed, efficiency, and accuracy (Truong et al. 2020). Unlike other systems, AI system has the capability to predict future cyber-attacks based on past threats, even if the threats changes (Zeadally et al., 2020). As a result, the use of artificial intelligence (AI) to combat security threats is unavoidable. In this paper our main goal is to highlight the importance of AI systems and technologies as a solution to cybersecurity (Fig. 1). How AI-based techniques can contribute to the protection of cybersecurity, is an important question to be answered through this paper. Furthermore, in this paper we have shown the limitations of AI in cybersecurity and some future research directions. The paper consists of sections arranged in the following order: Section 2 presents methodology related to literature review and search, Section 3 shows general background of AI techniques and applications in cybersecurity, Section 4 shows how AI can be applied on cybersecurity issues, Section 5 shows AI-based methods and techniques in cybersecurity, Section 6 highlights the benefits of AI in cybersecurity, Section 8 shows challenges of AI in cybersecurity, Section 9 is about discussion, Section 10 and 11 belongs to Future research directions and conclusion of the study.

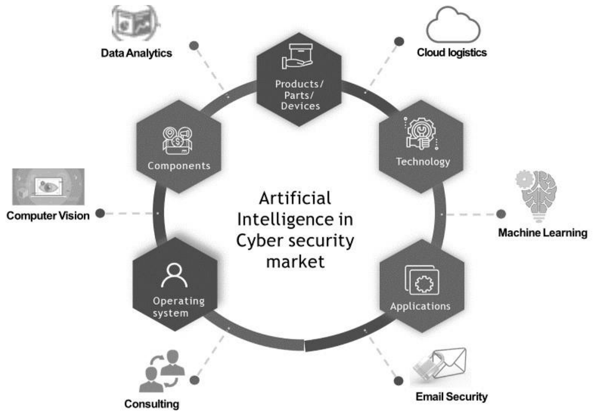

Figure 1. Application of Artificial Intelligence in cybersecurity market

2. Methodology

In this study we collected the manuscripts following a systematic methodology of literature review. The literature review was conducted focusing on the recent years. We selected recent time because of two reasons: 1. There are already numerous published articles available on internet regarding applications of artificial intelligence in cybersecurity, and 2. Our main objective is to shed light on the most recent and latest developments of artificial intelligence in cyber security. Literature search was performed using systematic approach (Fig. 2), in first step we searched and determined the most reliable search engines and databases for the literature. Then, in second step we designed the most specific and well-searched keywords with searchable filters related to the theme of the topic in this paper. With the help of these two steps, we created a downloaded literature library contained articles about recent developments of artificial intelligence applications in cybersecurity. We included those articles in the library containing the most up-to-date and closely related articles to our topic and these were used in the current paper. The following search engines and databases were searched to download the relevant articles: Google, Google scholar, Research gate, IEEE Xplore Digital Library, web of science, science direct, and Microsoft academic. All the papers were selected using criteria: Articles in English language, in prestigious journals, highly cited and easily accessible articles (e.g., available in PDF). The abstracts and conclusion sections of all related articles were scrutinized to make sure these are closely aligned with the topic of our study. Finally, we identify the future direction and challenges of the applications of artificial intelligence in cybersecurity.

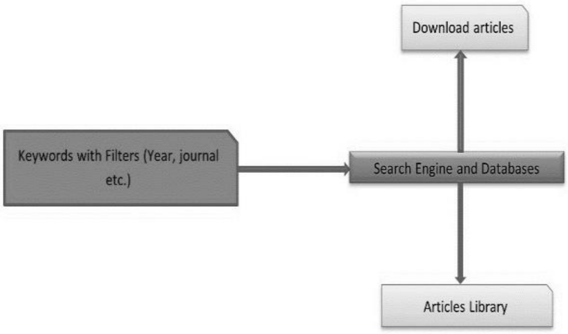
Download articles
Keywords with Filters (Year, journal etc.)
Search Engine and Databases
Articles Library

Figure 2. Methodology of literature collection and search

3. General background of AI techniques and applications in cybersecurity

With the rapid progress of internet technology and systems, the opposite is also true that cybercrimes and assaults are increasing at an alarming rate. To counter and defeat these cybercriminals and their smart techniques, we need AI-based techniques in our cybersecurity systems to enhance the cyberspace security more effectively. AI techniques and applications are presented briefly in Table 1.

Table 1. Techniques and applications of Artificial intelligence (AI) in cybersecurity

Techniques of AI	Applications in cybersecurity
Neural nets	1.For intrusion detection and prevention system 2.Very high-speed of operation 3.For Denial-of-service (DoS) detection 4.For forensic investigation 5.Warm detection 6.Fuzzy logic
Intelligent agents	1. Proactive and reactive 2. Agent communication language 3. Defense against Distributed Denial-of-service (DDoS)
Expert systems	1. For network intrusion detection 2. For decision support 3. Knowledge base 4. Inference engine
Application of Learning	1. Machine learning and deep learning 2. Data mining 3. Supervised and unsupervised learning 4. Intrusion detection and malware detection 5. Self-organizing maps

4. How AI can be applied on cybersecurity issues

AI provides several advantageous to deal with cybersecurity issues, some of the benefits AI provide are as follows:

(i) Unlike traditional technology which focused mainly on the past and totally depended on known cyber-attacks. If there is new cyber-attack happens the conventional systems are unable to detect the changes and thus leaving a blind spot during unusual attacks. AI can detect new and complex variations in attack flexibility (Tuang et al., 2020). In the future, AI systems will be more sensitive to detect similar changes (Tuang et al., 2020). The learning and adaptation capacity of AI machines is superior and can detect faster, anomalous, and more accurate operations. This ability of AI systems is more important when cyber-attacks are becoming more refined and cybercriminals are coming up with new and inventive methods (Truong et al., 2020).

(ii) AI has the ability to deal with large amounts of security data (Truong et al., 2020). Because AI includes self-contained security systems that can detect and respond to attacks. The amount of data breaches received daily is unbearable for security personnel; however, automatically detecting and responding to threats has helped to reduce experts' workload. Moreover, AI can better manage these cyberattacks than any other method. When a significant amount of security data is generated and transferred over the network daily, network security analysts will find it increasingly difficult to detect and monitor attack elements accurately and quickly. This is where AI can help by increasing the frequency with which suspicious type of behavior is mentioned and detected. This can assist network security officers in reacting to situations they haven't seen before, obviating the need for time-consuming people analysis.

(iii) Application behavior and regular network traffic are studied by AI security systems over time. In this way detecting the threats over time, AI make a baseline of what are the normal patterns. If any change or deviation found in the normal pattern, AI security system will detect the attacks.

5. AI techniques used for cybersecurity

Neural networks, expert systems, machine learning, deep learning, and data mining are just a few of the AI security models that can be used to effectively deal with cyberattacks and threats. AI-based methods can be used to make intelligent decisions in the cyberspace. In this paper we have highlighted all these AI techniques and described briefly in the following sections.

5.1. Artificial Neural Networks (ANNs)

Artificial Neural Networks (ANNs) was created by Frank Rosenblatt in 1957 as statistical learning technique that function like neurons in human brain (Mcculloch, & Pitts 1943). ANN technique mimicking neurons in terms of a mathematical equation where the model read enormous samples to produce a target value. ANNs are highly capable to understand, learn and solve the problems in different areas. It's also capable to solve noisy and incomplete data samples. In the cyber defense framework, ANNs have been used in the early warning phase, prevention phase, detection phase, and response phase (Kivimaa et al., 2008). ANNs are very useful in intrusion-detection systems (IDS) because of the adaptability. When used in cybersecurity, ANNs could be used to study traffic flow in security networks, allowing them to detect intrusions before they occur and then stop cyber-attacks through perimeter defense. (Bitter et al., 2010; Tyugu, 2011). ANNs have the potential to learn from past network activities to stop later threats. A typical illustration of ANN is shown in Fig (1).

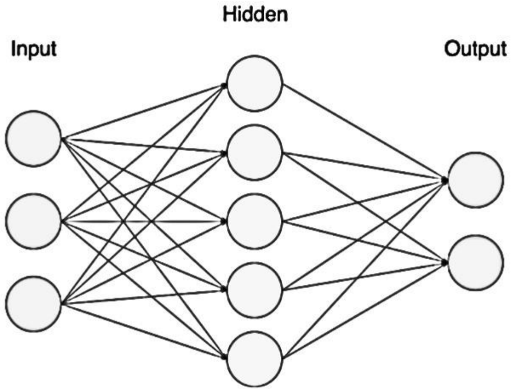

Figure 3. Typical Artificial Neural Network (ANN)

The Cascade Correlation Neural Network (CCNN) was used in a study of cybersecurity (Panchev et al., 2014), which stepwise adds new hidden units to the hidden layer. (Fahlman, & Lebiere 1990). When new events are detected, this system adds new hidden nodes to the network, training those nodes with the newly collected data. In this way CCNN provide runtime adaptive and scalable system. To learn from desktop-platform traffic patterns to detect port scanning to mobile networks, the CCNN only trains the network with new data, ignoring the entire network with the original data. The identification and evaluation of ANN port-scanning is analogous to other methods such as Decision trees, according to this investigation.

ANNs, in contrast to manual methods, have the ability to detect patterns in highly nonlinear problems with a high rate of classification (Stopel et al., 2009). Using previously transferred data over the network, ANNs can automatically place normal and abnormal network patterns. ANNS is used to scan network traffic by network security tools such as firewalls, network hubs, and intrusion detection systems. A more advanced form of ANN is Deep Neural Network (DNN), with high advantage it not only protects the security system from cyber-attacks, but also predicts that such attacks will occur in the future (Hinton et al., 2006). A study was carried out to detect cyber-attacks using DNN methods of AI-based security program, the results showed 85% success rate (Thomson, 2016). This achievement of DNN opened a new chapter of cybersecurity known as cyber-attack prediction.

5.2. Security Expert Systems

In AI, an expert system is a computer software application that assists a human expert in deciding. The system consists of two parts; knowledge base and inference engine, both collectively forms security rules (Tyugu, 2016). Cybersecurity expert system decisions are based on security guidelines. Expert systems modeling has applications in medical diagnosis, finance, and cyberspace. Expert systems are diverse, from small to large and complex hybrid systems which dealing with sophisticated issues and problems. The cybersecurity expert framework consists of a knowledge base phase which describe the knowledge of the domain as well as operational knowledge of the rules of security decisions, and the inference engine phase which is involved to get responses from the knowledge base and deduce new facts. Expert systems can be employed in different problems based on how the reasoning could be done. In one approach referred to as, "case-based reasoning (CBR) approach", a particular problem is solved by recollecting previous similar cases, then a solution is determined by adapting the past solution to a new problem case. In this way new solutions are analyzed to improve the accuracy and learning capacity of the system.

Rule-based systems (RBS) is another approach to solve problems, characterized by rules to solve problems defined by experts. The rule-based system consists of two sub-systems: condition part and the action. Condition part evaluation used to analyze the problems, then the action to be taken is determined. Cybersecurity expert system fighting against cyber-attacks using some guidelines and rules. For instance, it evaluates the process against the knowledge bae, if the process is good and known, then the security system considers it safe, if not the system declares it as a threat and then terminate the process. If the knowledge base lacks such a process, the system finds the sets of rules in the inference engine to determine the machine's state. The machine can be in one of three states: severe, moderate, or safe. The system notifies the manager or user of the machine's status based on the state of the machine, and then the inference as detected by the knowledge base.

A rule-based cybersecurity expert system model may thus have the decision-making capacity of a security expert in an intelligent cybersecurity framework built to solve complex cybersecurity issues, as well as by information reasoning. As a result, cybersecurity expert system modelling, based on its computing capabilities and ability to make intelligent decisions, can be a valuable component in AI-based cybersecurity.

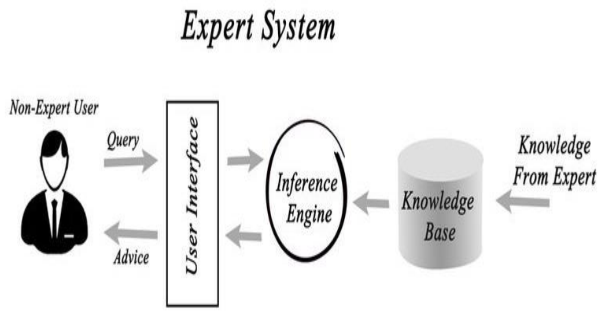

Figure 4. A typical Expert Security System

5.3. Intelligent agents (IAs)

Intelligent agents (IAs) are self-controlled systems with internal decision-making mechanism and a personal objective. It evaluates threats through sensors and monitor the domain via actuators. It controls the actions until a particular objective is achieved (Wirkuttis, & Klein 2017). These systems have proactive and responsive characteristics, and when communicating with other autonomous agents, can understand and respond to changes in their domain. In this way, these intelligent agents are adaptive in the sense these can learn and communicate with their environment. IAs are proved effective to stop Distributed Denial of Service (DDoS) attacks. How these agents can be used against distributed cyber-attacks? The answer is by constructing artificial "Digital police" which must include mobile intelligent agents, which obviously required to deploy infrastructure to provide firm support to the mobility and communication of cyber agents (Tyugu, 2016).

5.4. Search

Search is a critical thinking approach which can be employed in different situations especially when there is no alternate approach for critical thinking. We also using search strategy on daily basis as a subconscious problem-solving method. A prior knowledge about search strategy is required before performing search algorithm. These search algorithms have been embedded or added into almost every intelligent program and positively affecting the whole intelligent system. There are variety of methods of search security system in AI such as the αβ-search estimation which is employed as a part of various projects. The search estimation was created for computer chess. It employs the critical thinking strategy of "isolate and vanquish," which is particularly useful in primitive leadership when two foes are deciding on their most ideal activities. (Bhutada, & Bhutada 2018).

5.5. Bio-inspired Computing Method

Bio-inspired computing in AI is a newly emerged field consisting of smart algorithms and techniques that uses bio-inspired behaviors and attributes to tackle variety of academic and environmental sophisticated problems. Examples of bio-inspired computing techniques are Evolution Strategies (ES), Ant Colony Optimization (ACO), Artificial Immune System (AIS), Particle Swamp Optimization (PSO) and Genetic Algorithms (GA), these techniques are commonly employed in the cyberspace. This technique is also used in the classification of computer malwares. In the classification of computer malwares these techniques primarily used to optimize features and parameters for the classifiers. For example, PSO and GA techniques were employed to the improve the efficiency of malware detection system (AbRazak et al., 2018, Fatima et al., 2019). In another study fuzzy logic and GA were used for detection of intrusion (Ashfaq et al., 2017). The GA was used to create a digital signature of a network segment using glow analysis to predict network traffic behaviour for a specific time. In addition, the fuzzy logic method was used to determine whether or not an instance on the network was anomalous. The evaluation was conducted using network traffic from a university, and the results were 96.53 percent accuracy and 0.56 percent false notification.

5.6. Machine learning (ML) and Deep learning (DL) methods

Machine learning is a branch of AI that deals with teaching machines to learn new things and make decisions based on data using algorithms. Mathematical techniques that allow for the extraction of data, the discovery of patterns, and the drawing of conclusions from it are all closely related to machine learning. Classification and regression are the two most important methods of ML technology. 1. Supervised learning, 2. Unsupervised learning, 3. Semi-supervised learning, and 4.

Reinforcement Learning are all types of the ML technology.

Another learning known as deep learning is a knowledge about machine learning that uses data to train computers how to do things that previously only humans could do. This is accomplished by simulating the human brain's data interpretation mechanism. Deep learning is based on the principle that as we build larger neural networks and train them with more data, their performance improves.

ML and DL have been shown very important in resolving cybersecurity issues. ML methods have wider applications in the security system. Examples include spam filtering, network anomalies analysis, botnet tracking, and tracking user behavior anomalies. Similarly, DL has been proved effective in the detection of malware and network intrusions. S

6. Benefits of AI in cybersecurity

Those institutions implemented AI techniques in the cybersecurity operations have been benefited significantly (Lazic, 2019). For example, the ROI of some institutes have been increased by adopting AI in the cybersecurity issues. Siemens AG created AI based Siemens Cyber Defense Center (CDC) which is characterized by its high speed, self-controlled and adaptive. He used this system in Amazon Web Services (AWS). Due to AI application the system was estimated 60000 attacks per unit time. The overall capability was managed easily with less than 12 members as well good maintenance of system performance. AI in cybersecurity can identity new threats by analyzing previous threat patterns (Lazic, 2019). This approach of AI is useful to same time and energy used in the investigation and identification of threats and attacks. It has been revealed AI is very useful in the identification and reactions to threats with low cost (average of 12% cost reduction). Today, AI can provide enormous solutions to cybersecurity problems as the cybersecurity system is transforming from traditional and manual approaches towards automated algorithm mitigation. Unlike traditional technology which relies mostly on already identified intruders and intrusions and thus leaving a blind spot during unusual intrusion activities, AI can detect new, and complex change in the attack extensibility. These drawbacks of conventional security technology have now been resolved by AI technology. For example, privileged internet activities can now be monitored and any change in privileged access operations can be regarded as a potential threat. AI predictive methods offer an edge to security teams which is important to stop attacks before causing any destruction.

Dark trace (United Kingdom company) used ML technology for the detection of patterns and threats in many areas such as retails, manufacturing, energy, and transportation firms. Large amount of data and improvement of network security systems can be managed through AI-based techniques. The huge volume of active security issues is overwhelming for the security experts. Autonomous detection and response to attacks by AI has decreased the load of security groups. When security data in massive amount produced and transferred on daily basis, then it's a challenging task for the security experts to manage it.

Hence, AI can help to scale-up the analysis of doubtful processes and activities. Furthermore, the security personnel can take benefit and they can react to new situations better by replacing the manual methods which consume a lot of time when responding to novel situations. AI-based systems are ready to learn over time and can respond better to threats and attacks. AI help to identify attacks considering the characteristics of application and overall network activity. With the passage of time, AI memorized the normal and regular traffic status and set a limit for the normal activities. Hence, attacked is marked when there is any abnormal deviation.

7. Key challenges in AI-driven cybersecurity applications

The development of Artificial Intelligence system requires huge amount of data and input samples. It is evident collecting samples at this amount need lot of time to process and require lot of resources (i.e., memory and processing power etc.). The execution of AI technology requires costly and smart resources. End clients facing challenges in the frequent false alarm. False alarms have destructive effects on the essential responses which lead to disruption of entire business environment. Fine-tuning, a kind of trade off process, are used to decrease the false alarms and maintain the security level.

Intruders and attackers can employ different techniques such adversarial inputs, model theft and data poisoning to target and attack AI-based systems. An AI model comprised of four things such as perception of data, learning, fine decisions, and the ultimate actions. AI systems operating in a very sophisticated environment where all elements must interact and have mutual dependency. For example, a wrong perception can result wrong decision. Moreover, each of these elements are exposed to different attacks and threats. For instance, decisions are vulnerable to classic cyber-attacks and perception is exposed to training-attacks.

Finally, consistency concept is not logical. The prevention of system from misbehaving depends on the elements and these elements should be bounds to maintain lack of certainty. An efficient method is essential to separately verify the decisions, logic fixation and analysis of risk for corresponding elements of AI and ML. To fulfil the expectations of systems and reaction to variety of attacks new techniques are important to implement. The application of AI in cybersecurity area may produce new threats and thus the digital security can be in danger. The consistent detection and prevention of cyber-attacks by AI has also opened doors for attackers to develop more complex threats and attacks. One of the reason these attackers are motivated because the cost to develop technology decreases when access to AI techniques increases. This is possible that cyber criminals can develop more sophisticated and complex programs with the low amount. The rate of cybercrime has increased due to these factors. The human element of complacency is very important. In AI-based solutions to cybersecurity the risks of human element of complacency are poorly discussed. If institution follow AI and ML methods in cybersecurity, employees could be less conscious of prevention.

One of the greatest challenges in AI application in cybersecurity is the collection, management, and processing of unquantified data (structured, semi-structured, unstructured, or meta-data) especially when dealing the real-world cybersecurity problems (Sarker, 2021).

8. Discussion

In the current article, we have highlighted the potential applications of AI in the cybersecurity environment. AI providing various opportunities of investigations in the cyberspace. AI is the most effective system to combat against cyber-attacks due to their complexity, number, and flexibility. From the literature reviewed, it’s evident that AI-based methods can be employed to resolve cybersecurity issues in a very smart way unlike traditional security methods which are proved ineffective to work in the cyberspace. The continuous research in the AI applications in cybersecurity provide convincing evidence that AI is growing faster in terms of publications and with the passage of time more peoples will be focused on the AI applications in cybersecurity platform.

However, the other side of coin should also be considered while talking on the application of AI in cybersecurity. Four important factors which are employed by cyber-criminals must be considered before employing AI in cybersecurity: Adversarial threats, data poisoning and deception, stealing of models and false positive and negative. Despite of these limitations in AI applications, AI open new doors in the cybersecurity research.

9. Future research directions

The research work done so for shows Artificial intelligence techniques are vulnerable to adversarial attacks and this is one of the serious issues linked with security of data. AI techniques ignore and skip the traditional software analysis and proposed new attack vectors in the AI algorithms. Many of the applications can affect because of the hidden dependent features. For AI to be used as system element, a depth thorough research is required to develop engineering principles, new theories, and practices. Research required on safety of tools, threats modelling, vulnerability to the environment, and collaboration between human and machine. The designing of such models and techniques should be based on the expertise of AI. These models should repeatedly abstract and refine cyber-attacks. Moreover, the integrity and availability of data, control of data access, operation and privacy of networks, and plastic policy system should be considered.

10. Conclusion

With the rapid advancements of ICT, new challenges for cyber security have also evolved and emerged. Cyber-attacks and threats are now much complex and sophisticated that conventional techniques and approaches are uncapable to help further. These sophisticated cyber-attacks need new techniques and approaches which must be ideal, scalable, adaptable, and flexible. In this paper we have presented an overview of AI application in the cybersecurity. Some of the well-researched AI-based methods employed in the cybersecurity were discussed such as data learning, security expert systems and bio-inspired techniques. Furthermore, areas where AI playing role on cybersecurity are reviewed such as predication, detection, and prevention of intrusion and malware, barriers against distributed denial-of-service (DDos), a technique where digital police are deployed and many other areas. The advantages and some of the challenges of AI-based applications in cybersecurity were also discussed. These benefits include handling large volumes of data with high speed and accuracy, reduction in the cost while employing AI techniques in resolving cybersecurity issues and increased ROI on AI powered cybersecurity tools amongst others. Some of the key challenges using AI-based applications for cybersecurity are adversarial machine learning and self-approval by human beings. Nevertheless, AI-based security techniques are still used in the cybersecurity and there are more benefits than disadvantages. As humans are dependent on cybersecurity, many of the industry experts are agreed on the view that AI must be integrated with cybersecurity.

Acknowledgements.

I want like to express our gratitude to Professor Dr. Tao Feng, our project supervisor, for his unconditional support, instruction, and confidence.

References

[1] Ab Razak, M. F., Anuar, N. B., Othman, F., Firdaus, A., Afifi, F., & Salleh, R. (2018). Bio-inspired for features optimization and malware detection. Arabian Journal for Science and Engineering, 43(12), 6963-6979.

[2] Ashfaq, R. A. R., Wang, X. Z., Huang, J. Z., Abbas, H., & He, Y. L. (2017). Fuzziness based semi-supervised learning approach for intrusion detection system. Information Sciences, 378, 484-497.

[3] Atiku, S.B., Aaron, A.U., Job G.K., Fatim, S., & Yakubu, I.Z. (2020). Survey On the Applications of Artificial Intelligence in Cyber Security. International Journal of Scientistic and Technology Research, 9(10), 165-170.

[4] Bhutada, S., & Bhutada, P. (2018). Applications of Artificial Intelligence in Cyber Security. International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), 5(4), 214-219.

[5] Bitter, C., Elizondo, D. A., & Watson, T. (2010, July). Application of artificial neural networks and related techniques to intrusion detection. In The 2010 International Joint Conference on Neural Networks (IJCNN) (pp. 1-8). IEEE.

[6] Fahlman, S. E., & Lebiere, C. (1990). The cascade-correlation learning architecture. CARNEGIE-MELLON UNIV PITTSBURGH PA SCHOOL OF COMPUTER SCIENCE.

[7] Fatima, A., Maurya, R., Dutta, M. K., Burget, R., & Masek, J. (2019, July). Android malware detection using genetic algorithm based optimized feature selection and machine learning. In 2019 42nd International conference on telecommunications and signal processing (TSP) (pp. 220-223). IEEE.

[8] Helm, J. M., Swiergosz, A. M., Haeberle, H. S., Karnuta, J. M., Schaffer, J. L., Krebs, V. E., ... & Ramkumar, P. N. (2020). Machine learning and artificial intelligence: definitions, applications, and future directions. Current reviews in musculoskeletal medicine, 13(1), 69-76.

[9] Hinton, G. E., Osindero, S., & Teh, Y. W. (2006). A fast learning algorithm for deep belief nets. Neural computation, 18(7), 1527-1554.

[10] Kabbas, A., Alharthi, A., & Munshi, A. (2020). Artificial intelligence applications in cybersecurity. IJCSNS International Journal of Computer Science and Network Security, 20(2), 120-124

[11] Kivimaa, J., Ojamaa, A., & Tyugu, E. (2008, October). Graded security expert system. In International Workshop on Critical Information Infrastructures Security (pp. 279-286). Springer, Berlin, Heidelberg.

[12] Lazic, L. (2019). Benefits from AI in Cyber Security. The 11th international Conference on Business Information Security. Belgrade, Serbia (pp. 1-9).

[13] McCulloch, W. S., & Pitts, W. (1943). A logical calculus of the ideas immanent in nervous activity. The bulletin of mathematical biophysics, 5(4), 115-133.

[14] Morgan, S. (2019). Global cybersecurity spending predicted to exceed $1 trillion from 2017-2021. Cybercrime Magazine, 10. https://cybersecurityventures.com/cybersecurity-market-report/ (Accessed: August 7, 2021).

[15] Panchev, C., Dobrev, P., & Nicholson, J. (2014, September). Detecting port scans against mobile devices with neural networks and decision trees. In International Conference on Engineering Applications of Neural Networks (pp. 175-182). Springer, Cham.

[16] Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. SN Computer Science, 2(3), 1-21.

[17] Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2(3), 1-18.

[18] Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. Journal of Digital Forensics, Security and Law, 12(2), 8.

[19] Shamiulla, A.M. (2019). Role of Artificial Intelligence in Cyber Security. International Journal of Innovative Technology and Exploring Engineering, 9(1), 4628-4630.

[20] Soni, V. D. (2020). Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. Available at SSRN 3624487.

[21] Srivastava, S., Benny, B., Ma'am, M. P. G., & Ma'am, N. B. (2021). Artificial Intelligence (AI) and It's Application in Cyber Security (No. 5791). EasyChair.

[22] Stopel, D., Moskovitch, R., Boger, Z., Shahar, Y., & Elovici, Y. (2009). Using artificial neural networks to detect unknown computer worms. Neural Computing and Applications, 18(7), 663-674.

[23] Thomson, V. (2016, April 21). Cyber Attacks could be predicted with Artificial Intelligence Help. PatternEX News.

[24] Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial intelligence in the cyber domain: Offense and defense. Symmetry, 12(3), 410.

[25] Truong, T. C., Zelinka, I., Plucar, J., Čandík, M., & Šulc, V. (2020). Artificial intelligence and cybersecurity: Past, presence, and future. In Artificial intelligence and evolutionary computations in engineering systems (pp. 351-363). Springer, Singapore.

[26] Tyugu, E. (2011, June). Artificial intelligence in cyber defense. In 2011 3rd International Conference on Cyber Conflict (pp. 1-11). IEEE.

[27] Wirkuttis, N., & Klein, H. (2017). Artificial intelligence in cybersecurity. Cyber, Intelligence, and Security, 1(1), 103-119.