IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 10, Issue 1, January 2020, ||Series -III|| PP 45-48

A Survey on different techniques in Artificial Intelligence that can be enforced in cybersecurity

Nikhil S.Band, Shilesh P.Thakare, Avinash G.Mahalle
Assistant Professor Department. of Information Technology PRMIT & R,Badnera Amravati,India
Assistant Professor Department. of Information Technology PRMIT&R,Badnera Amravati,India
Assistant Professor Department. of Information Technology PRMIT&R,Badnera Amravati,India
Received 01January 2020; Accepted 15 January 2020

Abstract— AI is a branch of Computer Science concerned with the study and creation of computer systems.AI is a study of how to make computers do things which at a moment, people do better. Today businesses using modern technologies like cloud, big data, mobile, and social media. Although these technologies unlock a whole new set of capabilities and rewards for businesses, they also expose them to to hitherto unknown risks. when hackers would deploy adware, malware, Trojan viruses, phishing attacks or standard keyloggers on private systems for small gains, the focus of hackers and cybercriminals has shifted from individual users to big businesses and corporations since they make for more lucrative targets. But financial rewards are not the only motive behind cyber-attacks. Gaining access to sensitive data and using it for illegal purposes, cause enterprises far more damage, not only in terms of financial losses but also hurting the reputation they have painstakingly built over several years. now, before cyberattack occurs it will be prevented by using modern technology. This paper proposes techniques to prevent cyber attacks by the development of cybersecurity skills and how artificial intelligence can be implied to improve skills through the use of artificial neural networks and machine learning algorithms.
Keywords— Artificial Intelligence, Cybercrime, Cyber-attacks, Cyber Security, Artificial Neural Networks and Machine Learning Algorithms.

I. INTRODUCTION

Artificial intelligence (AI) is the simulation of human intelligence processes by machines, especially computer systems. These processes include learning (the acquisition of information and rules for using the information), reasoning (using rules to reach approximate or definite conclusions) and self-correction. In another word the importance of artificial intelligence is the ability to create a never-ending thought process and collective that could solve our problems. Accomplishing this by thinking of every possible solution. For modern enterprises, the road to digital transformation is fraught with several obstacles, most notably, those concerning the issue of cybersecurity. Today, when we talk about cybersecurity threats, it's more a question of 'when', rather than 'if', an attack will occur. This is true especially in a time when enterprises around the world are shifting their focus towards achieving greater mobility and connectivity of technologies with the help of cloud applications and infrastructures, Internet of Things (IoT), etc. to help them achieve the level of efficiency they require.

Artificial Intelligence (AI) is now at the center of the cybersecurity industry. Artificial intelligence is a term that is relatively over these days, but it actually refers to a few techniques that can be very valuable for security. It consists of machine learning algorithms that can identify and respond to threats as they occur. They can predict whether incoming data are potentially malicious or safe. Many attacks that happen in these days are not new. In fact, these attacks have happened to some other people in some other places before. Thus, if we establish a database that collects all the information that has ever occurred and feeds it to machine algorithms, attacks can be prevented before they occur.

In classification one, we can look at the features of the data to decide whether or not it is malicious. Other techniques involve detecting anomalies in the processing of data quickly in real time, so that incoming data is treated as a stream that collects every single point and then uses an algorithm that can track what standard of behavior that appears to be normal and looks at deviations that could mean that there has been a hack or intrusion. And then there is a third one which uses a technique called probabilistic programming. This is a set of computer languages that do not write a computer program with deterministic rules but can distribute probabilities and there is some very interesting research in analytics to actually do a whole genealogy of malware so that we can track the history of these infectious viruses to inform future responses.

Neural networks and deep learning algorithms can process a lot of data quickly and discern features of all sorts of things, whether the images or texts on the internet and use these features to decide whether or not the data is malicious. Using past data, they can learn and never make mistakes again. It is complex and difficult for

humans to interpret neural networks. The output is not concrete. Therefore, the traditional security solution is declining. The use of AI in cybersecurity increases speed and scalability [2].

II. RELATED WORK

Swapnil Ramesh Kumbar [4] has proposed a system that uses fuzzy system techniques, pattern recognition, image processing, and data mining techniques. Phishing and fake auctioning can be prevented with Data Mining. Pattern matching uses fingerprinting, facial recognition, voice recognition as security, image processing is mainly used in defense and military, fuzzy logic is mainly used when malware invasion takes place.

Mohana K.V et al. [5] have proposed a system that uses data security, the Chaotic Neural Network and the use of genetic algorithms for data security. Random numbers are generated using a Generic Algorithm and passed as a parameter used in the processing of the neural network. After processing the neural network, a key is produced that is used for encryption. If we reverse the above process decryption takes place. It is not easy to decrypt the data.

Selma Dilek et al. [6] have proposed a system that uses artificial immune systems, ontology, general intelligence. The air-based email system is used for spam encounter. The ontology represents knowledge and general intelligence uses strong AIs.

Alberto Perez Veiga [7] has proposed a system that uses machine learning technology. Although AI is not used as expected in the field of cybersecurity, machine learning is successfully used to solve small parts of the complex problems.

Ranjeev Mittu et al. [8] have proposed a system that uses technologies to detect advanced persistence threats. The system addresses ubiquitous cyber threats and the role of hackers and users.

Enn Tygu [9] has proposed a system that uses applications based on neural networks and techniques used in cyber defense. In this system, the constraint solving technique is used to find solutions to the constraints of the given problem solution. The neural network is not suitable for all areas. Therefore, an application can be used as a defense method where the neural network is not efficient.

III. COMPARISON OF DIFFERENT CYBERSECURITY IN AI

Sr.No	Approach	Methods	Result	Advantages	Ref. No
1	Survey and analyzing different methods for improving cybersecurity with the use of AI	Expert Systems, Neural Networks, Intelligent Agents	improving security with the use of Artificial Intelligence	Increase accuracy and efficiency of Intrusion Detection	#3
2	Overview of different techniques in AI that can be implemented in cybersecurity	Artificial neural networks, Image processing, data mining, fuzzy system, expert system, pattern recognition	Increasing the performance of security systems using different AI techniques	Can adapt to different situations, help with decision making, accurate and quick	#4
3	Using a genetic algorithm for optimization problems	An artificial neural network, Chaotic neural networks, encryption, decryption, security.	Encryption and Decryption of original data by using chaotic neural networks and genetic algorithms	Ensures optimal security when compared to open channels	#5
4	Study and demonstrate different AI methods	The artificial immune system, Intelligent Agents,	Techniques used in applications to combat cybercrime	Non- linearity, mobility, dynamic structure,	#6

	for combating cyber attacks	Fuzzy sets, Genetic algo.		resilience, versatility	
5	Provides usage of AI in network security and informs about the evolution of cybersecurity	Artificial Intelligence with Machine learning	Usage of ML in cybersecurity provides reactive real-time security	Real-time effective protection again cybercrime	#7
6	Engineering approaches to mitigate cyber threats using AI	Artificial Intelligence	Advance persistence threats are difficult to detect so using of AI becomes necessary	AI application are present which can detect and continue future threats	#8
7	Provides a survey of Artificial Intelligence methods used in cyber defense	Neural nets, Expert system, Intelligent agents	Application based on neural networks are used in cyber defense	Development in AI applications will help decrease cyber threats in the world	#9
8	Introducing in an advance cybercrime defense system involving Artificial Intelligence agents	Intrusion detection and prevention system, Artificial agents, Intelligence agent	Provides information about the cybercrimes and advances made using AI with a security system	Tracing the attacker and responding to the source can be done in the most efficient way using Artificial Intelligence	#10

IV. DISCUSSION

AI is the study of creation of machine that behave like human, actually creation of intelligent program that run on machine. we efficiently and accurately secure our network by using latest technologies. The Technologies are expert systems, intelligent agents etc.

V. CONCLUSION

The main purpose of data security is securing valuable data from unauthorized use. The main role of AI is to warn people before hacking.AI use some of the technology to protect the data from unauthorized use in this way AI plays an important role in data security. This paper suggests different techniques in Artificial Intelligence that can be enforced in cyber security . some of the techniques are expert systems, neural networks, and intelligent agents. In AI Machine is not intelligent human provide knowledge to machine and machine only follow instruction due to this continuous human interactions and training is need when AI uses machine learning, deep learning, etc.

REFERENCES

[1]. AI and security -https://www.youtube.com/watch?v=ojTz7bOjT6o&t=87s
[2]. How ML and AI will increase cyber security (a webinar)-https://www.youtube.com/watch?v=lO2Cf5BmjvI
[3]. Harini M Rajan, Dharani S "Artificial Intelligence in Cyber Security-An Investigation" Int. Res. J. Comput. Sci. Issue, vol. 09, no. 4, pp. 28–30, 2017.
[4]. Swapnil Ramesh Kumbar "An Overview on Use of Artificial Intelligence Techniques in Effective Security Management," Int. J. Innov. Res. Comput. Commun. Eng. (An ISO, vol. 2, no.9, pp. 5893–5898, 2014.
[5]. Mohana,K.V.K. Venugopal, Sathwik H.N. "Data Security using Genetic Algorithm and Artificial Neural Network," Int. J. Sci. Eng. Res., vol. 5, no. 2, pp. 543–548, 2014.

[6]. Selma Dilek, Huseyin Cakir and Mustafa Aydin "Applications of Artificial Intelligence Techniques to Combating Cy ber Crimes: A Review," Int. J. Artif. Intell. Appl., vol. 6, no. 1, pp. 21–39, 2015.
[7]. Alberto Perez Veiga "Ap p lication of Artificial Intelligence (AI) to Network Security " ITEC 625 – Information Systems Infrastructure, 2018.
[8]. Ranjeev Mittu & Willliam F. Lawless, "Human Factors in Cybersecurity and the Role for AI," in Foundations of Autonomy and Its (Cyber) Threats: From Individuals to Interdependence: Papers from the 2015 AAAI Spring Symposium, 2015, pp. 39–43.
[9]. Enn Ty ugu "Artificial Intelligence in Cy ber Defense"2011 3rd International Conference on Cyber Conflict.
[10]. L.S.Wijesinghe,L.N.B De Silva, G.T.A.Abhayaratne, P.Krithika, S.M.D.R. Priyaashan, Dhishan Dhammeratchi "Combating Cy ber Crime Using Artificial Agent Sy stems," Int. J. Sci. Res. Publ., vol. 6, no. 4, pp. 265–271, 2016.
[11]. Arockia Panimalar.S, Giri Pai.U, Salman Khan.K, "Artificial Intelligence Techniques for Cyber Security," Int. Res. J. Eng. Technol., vol. 5, no. 3, pp. 122–124, 2018. 12. Anna L. Buczk, Erhen Guven, "A Survey of Data M ining and Machine Learning Methods for Cyber Security Intrusion Detection," IEEE Commun. Surv. Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.
[12]. Anna L. Buczk, Erhen Guven, "A Survey of Data M ining and Machine Learning Methods for Cyber Security Intrusion Detection," IEEE Commun. Surv. Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.
[13]. Nikhil.S.Band, " Role of Artificial Intelligence, Cloud and Internet of Things to Become Smart City Secure and Safe-a Review" 61st IETE Annual Convention 2018 on "Smart Engneering for Sustainable Development Special Issue of IJECSCSE, ISSN:2277-9477

Nikhil S.Band,et.al. "A Survey on different techniques in Artificial Intelligence that can be enforced in cybersecurity" *IOSR Journal of Engineering (IOSRJEN)*, 10(1), 2020, pp. 45-48.