Available online at: http://www.ijmtst.com/vol5issue12.html

International Journal for Modern Trends in Science and Technology

ISSN: 2455-3778 :: Volume: 05, Issue No: 12, December 2019

# Artificial Intelligence Techniques to Prevent Cyber Attacks

Amit Dua[1] | Chandra Prakash[2] | Rakesh Kumar Saini[3]

[1,2,3]Department of Computer Science & Application, DIT University, Dehradun, Uttrakhand, India

**To Cite this Article**

Amit Dua, Chandra Prakash and Rakesh Kumar Saini, "Artificial Intelligence Techniques to Prevent Cyber Attacks", *International Journal for Modern Trends in Science and Technology*, Vol. 05, Issue 12, December 2019, pp.-09-12.

**Article Info**

Received on 07-November-2019, Revised on 21-November-2019, Accepted on 27-November-2019, Published on 30-November-2019.

## ABSTRACT

*Modern innovations in ArtificialIntelligence is proving to be the best option in defending cyber-attacks. Artificial intelligence (AI) and its subset machine learning are being used by experts as a means to fight against cyber- attacks. Currently, security analyst use this technology to flag anomalies, saving time and also cutting overall businesses costs. In this digital world, with the outburst of IOT and linked devices, cyber security experts face a lot of encounters. The expert needs all the means to prevent attacks and security cracks and respond to the attacks. Where conventional security systems may be less competent and deficient, artificial intelligence techniques can enhance their overall security execution and give better security from an expanding number of complex cyber threats. In this paper we basically look howhuman reasoning along with AI can be applied to uplift cyber security. The main purpose of this study is to present advances made so far in the field of applying AI techniques for combating cyber-attacks.*

***KEYWORDS:*** *Cyber security, Artificial Intelligence (AI), Security intelligence, Cyber defense.*



## I. INTRODUCTION

Artificial Intelligence is the ability to think, to understand, to recognize patterns, to memorize, to make choice from alternatives and to learn from experience. Artificial Intelligence is to make replica of human brain's capabilities so that the computers start doing all those activities that the human is doing and in much less time. The recent developments in AI affected politics, journalism, games and public life. In politics the use of Artificial Intelligence helped to better use of resources, energy and time in the election campaign to reach the target audience. Cyber-attacks are threats to governments, businesses, and institutions today. Data Breaches at the Federal Bureau of Investigation (FBI) and Department of Homeland Security exposed around 200 million personal records including high-profile data leaks.AtPresents it's just trying to figure out what other humans are trying to do which is slow and limited. The global market for cyber security is estimated to reach 170 billion by 2020 according to a Forbes report. The main reason for the rapid market bump is rising technology trends and the blitz of initiatives that keep security requirements evolving. Cyber security is the buzzword right now and lately; it is being used with Artificial Intelligence. Artificial Intelligence enabled cyber security programs are proving to be better at protecting and safeguarding digital information. Artificial Intelligence can play a vital role in helping with such threats. Artificial Intelligence is capable of being a valuable ally when it comes to

establishing a line of defence against hackers. Artificial Intelligence can be trained to detect and learn patterns continually for any deviation in it. Machine learning is a crucial component of Artificial Intelligence. It uses collected data to constantly improve its functions and develop preventive strategies to tackle future attacks. Its ability to learn and understand user behavior and recognize patterns and identify slightest deviations in those patterns makes it perfect for Cybersecurity. Additionally, Artificial Intelligence can use this information and develop its own strategies and functions as well [1][2]. The main goal of Artificial Intelligence is to create a technology that allows computers and machines to function in an intelligent manner. From a cybersecurity perspective, AI can be utilized as a tool to quickly and accurately identify new vulnerabilities in an effort to mitigate future attacks. This technology can alleviate much of the burden currently being placed on human security workers who are overworked, limited by human capabilities and inevitably proneto error. With a cyber-security strategy that's powered by intelligentautomation, machines do much of the heavy lifting, alerting human agents only when action is needed. This enables security personnel to allocate their time and skills more effectively. In this paper we highlight the deficiencies of conventional security measures and additionally the advance that has been made so far by applying Artificial Intelligence techniques to cyber-attack[3][4].

## II. ARTIFICIALINTELLIGENCE APPLICATIONS

Artificial Intelligence is playing a major role in revolutionizing a number of industries. Some reports have suggested that the total global market for Robots and Artificial Intelligence will reach ~$153 billion by 2020. Artificial Intelligence not only decreases costs but also saves time, increases accuracy and productivity. The development in the field of Artificial Intelligence has been phenomenal. Google estimates that robots will reach levels of human intelligence by 2015, one-third of jobs will be replaced by robots and other smart machines[5].

### *A. Artificial Intelligence Inhealthcare*

The biggest bets are on improving patient outcomes and reducing costs. Companies are applying machine learning to make better and faster diagnoses than humans. One of the best known healthcare technologies is IBM Watson.It understands natural language and is capable of responding to questions asked of it. The system mines patient data and other available data sources to form a hypothesis, which it then presents with a confidence scoring schema. Other AI applications include chatbots, a computer program used online to answer questions and assist customers, to help schedule follow-up appointments or aid patients through the billing process, and virtual health assistants that provide basic medical feedback [6].

### *B. Artificial Intelligence inbusiness*

Robotic process automation is being applied to highly repetitive tasks normally performed by humans. Machine learning algorithms are being integrated into analytics and CRM platforms to uncover information on how to better serve customers. Chatbots have been incorporated into websites to provide immediate service to customers. Automation of job positions has also become a talking point among academics and ITanalysts.

### *C. Artificial Intelligence ineducation*

AI can automate grading, giving educators more time. AI can assess students and adapt to their needs, helping them work at their own pace. AI tutors can provide additional support to students, ensuring they stay on track. AI could change where and how students learn, perhaps even replacing someteachers.

### *D. Artificial Intelligence infinance*

Artificial Intelligence in personal finance applications, such as Mint or Turbo Tax, is disrupting financial institutions. Applications such as these collect personal data and provide financial advice. Other programs, such as IBM Watson, have been applied to the process of buying a home. Today, software performs much of the trading on WallStreet.

### *E. Artificial Intelligence in law*

The discovery process, sifting through of documents, in law is often overwhelming for humans. Automating this process is a more efficient use of time. Startups are also building question-and-answer computer assistants that can sift programmed-to- answer questions by examining the taxonomy and ontology associated with adatabase.

### *F. Artificial Intelligence in manufacturing*

This is an area that has been at the forefront of incorporating robots into the workflow. Industrial

robots used to perform single tasks and were separated from human workers, but as the technology advanced thatchanged.

*G. Artificial Intelligence in CyberSecurity*

Artificial Intelligence can play a vital role in helping with such threats. Artificial Intelligence is capable of being a valuable ally when it comes to establishing a line of defence against hackers. AI can be trained to detect and learn patterns continually for any deviation in it [7].

## III. ADVANTAGESOF ARTIFICIAL INTELLIGENCE

Organizations face millions of threats each day making is impossible for a security researcher to analyze and categorize them. This task can be done by using Machine Learning in an efficient way. By finding a way to work towards unsupervised and supervised machine learning will enable us to utilize our current knowledge of threats and vectors fully. Once those are combined with the ability to detect new attacks and discover new vulnerabilities, our systems will be able to protect us from threats is a much better and efficientway.

*A. ErrorReduction*

We use artificial intelligence in most of the cases. As this helps us in reducing the risk. Also, increases theChance of reaching accuracy with the greater degree of precision.

*B. DifficultExploration*

In mining, we use artificial intelligence and science of robotics. Also, other fuel exploration processes. Moreover, we use complex machines for exploring the ocean. Hence, overcoming the oceanlimitation.

*C. DailyApplication*

As we know that computed methods and learning have become commonplace in dailylife.

Financial institutions and banking institutions are widely using Artificial Intelligence. That is to organize and manage data. Also, Artificial Intelligence is used in the detection of fraud users in a smart card based system[8].

*D. DigitalAssistants*

“Avatars” are used by highly advanced organizations. That are digital assistants. Also, they can interact with the users. Hence. They are saving human needs of resources. As we can say that the emotions are associated with mood. That they can cloud judgment and affect human efficiency. Moreover, completely ruled outfor machineintelligence.

*E. Nobreaks*

Machines do not require frequent breaks and refreshments for humans. As machines are programmed for long hours. Also, they can continuously perform without getting bored[9].

*F. Increase WorkEfficiency*

For a particular repetitive task, AI-powered machines are great with amazing efficiency. Best is they remove human errors from their tasks to achieve accurateresults.

*G. Reduce cost of training andoperation*

Deep Learning and neural networks algorithms used in Artificial Intelligence to learn new things like humans do. Also, this way they eliminate the need to write new code every time[10]

## IV. ARTIFICIAL INTELLIGENCE IS THE FUTURE OFCYBER-SECURITY

Cyber-attack is one of the biggest threats to businesses, governments, and institutions today. More than 200 million personal records were exposed in data breaches in 2016; including high-profile breaches at the Department of Homeland Security and the Federal Bureau of Investigation (FBI).99 percent of exploited vulnerabilities are already known. Unfortunately, we tend to rely on firewalls as a defence. But firewalls will not stop a determined hacker. For now, it’s just humans who try to anticipate what the other human might do before they do it [11][12]

When we say ArtificialIntelligence, your mind probably goes right to the Terminator movies and SkyNet. When I first saw that movie I ruined a good pair of pants and spent the next few months in adult diapers while I waited for the flashbacks to stop. So you can probably imagine how many Tide pods it took to rectify my reaction when I saw AI and Machine Learning (ML) in the news recently. When it comes to Artificial Intelligence and Machine Learning, no industry is left impacted, including the cybersecurity. There are series of cybersecurity companies- start-ups and established started producing AI integrated products helping to secure data from third-party clients. From AI mobile app development to Blockchain Development, everything requires the cybersecurity roof and AI is playing a major role [13].

## V. CONCLUSION

Artificial Intelligence is adding values to the security sectors of the corporations and individuals as well, it is also spreading more power in the wrong hands. In order to give Artificial Intelligence more authority in the near future for the security purposes, we need to stay sure that it stays with the white hat people only. There is no doubt that artificial intelligence is limitless and smart and faster than human, but it requires human touch to get going. So businesses need to focus largely on hiring and training Artificial Intelligence experts who can work with the machine for product safety. Combining of the human mind and AI will certainly help in fighting against the hackers. In conclusion, artificial intelligence is beginning to play an increasingly important role in how organizations keep their networks and sensitive data secure. In the not-so-distant future, advances in machine learning, AI and intelligent automation will continue to provide newer, better and more effective tools to help savvy organizations stay a step ahead of cybercriminals.

## REFERENCES


[1] Anderson, Frivold, Valdes, "Next- Generation Intrusion Detection Expert System(NIDES)".

[2] B. Iftikhar, A. S. Alghamdi, "Application of artificial neural network within the detection of dos attacks",2009.

[3] P. Norvig, S. Russell. "Artificial Intelligence: fashionable Approach",2000.

[4] E. Tyugu. Algorithms and Architectures of Artificial Intelligence. IOS Press.2007.

[5] NabaSuroor and Syed Imtiyaz Hassan, "Identifying the factors of modern day stress using machine learning", International Journal of Engineering Science and Technology, vol. 9, Issue 4, April 2017, pp. 229-234, e-ISSN: 0975–5462, p- ISSN:2278–9510.

[6] Syed Imtiyaz Hassan, "Designing a flexible system for automatic detection of categorical student sentiment polarity using machine learning", International Journal of u- and e- Service, Science and Technology, vol. 10, no.3, Mar 2017, pp. 25-32, doi: 10.14257/ijunesst.2017.10.3.03, ISSN: 2005- 4246.

[7] Syed Imtiyaz Hassan, "Extracting the sentiment score of customer review from unstructured big data using Map Reduce algorithm", International Journal of Database Theory and Application, vol. 9, issue 12, Dec 2016, pp. 289-298, doi: 10.14257/ijdta.2016.9.12.26, ISSN:2005-4270.

[8] C2-level Security, [Online: Available], https://msdn.microsoft.com/enus/library/windows/desktop/aa376387 (v=vs.85).aspx.

[9] J. Beal, P. H. W inston, "Guest Editors' Introduction: The New Frontier of Human-Level Artificial Intelligence", Intelligent Systems, IEEE 24.4: 21-23,2009.

[10] Sivarajah, U., Kamal, M.M., Irani, Z. and Weerakkody, V. (2017). Critical Analysis of Big Data Challenges and Analytical Methods, Journal of Business Research, 70, 263-286.

[11] Hernándeza, Á.B., Perez, M.S., Gupta, S., Muntés-Mulero, V. (2018). Using machine learning to optimize parallelism in big data applications, Future Generation Computer Systems, 86, 1076- 1092.