ISBN: 978-93-92995-10-1

ARTIFICIAL INTELLIGENCE IN CYBER-DEFENSE TECHNOLOGIES

JAYADEV C.K

KEVIN GLADIUS
Email ID: jayadev.ck2018@vitstudent.ac.in

Abstract
One of the most important things in the world, today is privacy. More than essential things such as food, shelter, etc., people need to worry more about invasion of their private life. With the advancement of technologies to provide us more comfort in our lives, even the bad side of it has surfaced more. Hackers use more complex algorithms to crack a network and steal very sensitive and confidential data, which might affect a single person or sometimes as large as a country. In this paper, we are going to see about the importance of cyber security and the various technologies involved in it and also how the advancement of artificial intelligence, machine learning and its related concepts improve cyber-defense. Every technology has drawbacks. So we will also look into the different issues we face while using AI including the risks in using them too. While trying to prevent network intrusion, we leave all our information to a software which is unpredictable and difficult to comprehend how it thinks.
***Keywords**: Artificial Intelligence, AI, Cyber-Defense, Privacy, Network Intrusion, Cyber security, Machine Learning*

Introduction

The seamless connectivity between the systems of the dynamic world needs a very effective defense system. The technologies involved are progressively improving day by day with the increasing demand for privacy, money policy, information sharing and so on. 'Artificial Intelligence' is a boon for the cyber- security companies to provide the user everything mentioned above. Why is this required? The human mind is not capable of performing various complex tasks at the same time. The various ways in which an infiltrator might breach into a secured system is an example of a situation like that. AI will take care of this by reading through all possibilities of a breach by using concepts such as brute force protection in real time. This will not only help in getting rid of an individual's cyber risks but also protecting the ultra-sensitive information possessed by organizations, governments, and armies which shouldn't be leaked to the general public. The complete avoidance of human intervention can lead to improved defensive technologies like detection and prevention of network intrusion and fraud, botnet detection, an eye over hacking entities and much more. is all possible due to the of AI as these algorithms concepts like computational, fuzzy logic, intelligent agents, immune systems, data mining, pattern recognition, etc., In the year 2016, almost 3 billion accounts of 'Yahoo!' were compromised conveying all information such as email addresses, passwords, date of birth and contact information to the netizens thereby flooding the internet. Incidents like these can be avoided if there was an active supervision on all gateways that are breachable and a swift response to any breach by quarantining any malware present. This paper will feed you all the information about how these kinds of issues can be resolved using Artificial Intelligence and will give you more insight about cybersecurity needs and demands and also the disadvantages of involving AI in catering these needs.

Literary Survey

[1] There are a lot of different ways in which cyber security can be boosted with the help of computational intelligence. Some of which are fuzzy logic, artificial immune systems, neural networks, machine learning, etc., But any cyber defense system can't beat the human immune system. The mechanism in which our body works to defend our system is so perfect that its quite impossible to mimic it into an algorithm but at least some concepts injecting vaccine so that our body can learn how to attack a pathogen can be taught to a computer hence forming a more capable defense system.[2] Many problems occur in the world of the internet. In brief it can be listed as in five ways, firstly the problem cyber threats making the life of common people hectic. The advanced persistent threats which can even provoke a situation of national security.The lack of research in the field poses a huge problem as no one knows what is happening to their system. The only way to solve such threats is to improve the technology of artificial intelligence and implementing in the domain of security.[3] On implementing artificial intelligence in cybersecurity there would obviously be problems waiting to attack the developer. But what if the problem was not on implementation and what if there was a problem but the AI fixes it on its own, meaning the systems is completely functioning on its own then who is governing its actions. The concept of psychopathology is used in this kind of cases. There would always be some kind of fault modes in an intelligent machine, maybe some kind of interpretation is wrong or the process is done for a different application entirely or there is an entirely a different kind of problem. When this type of problems arises is it right to let the AI to function on its own and fix it? These types of problems are new and requires a lot of research in the field such as" psychopathology of AI" as this is not just about an AI but it also concerns for the use of cybersecurity as well.[4] Along the advancing of artificial intelligence implemented in cyber defense, the different types of problems that occur also tend to improve. One of them is the DDos attacks or 'distributed denial of service' attacks. Basically, these programs get inside a network and start putting up unnecessary authentication of accessing data that might even be visible publicly and ultimately disable the entire network system. So, problems like these arise every now then but solutions are also created, might not be immediate but very soon. Like this there are many obstructions to improvement and to cross all these obstructions AI seems to be the answers by many developers because the use of machine learning under AI will never fail to succeed if implemented properly. Learning how the attacks happen and how to stop a malware will eventually beat it.[5] Cyberbullying can be seen an aftereffect of one's cyber defense system fails to tackle a malware or a break in. Many different people and companies are affected by this means, leaving their private information in jeopardy to the open internet. Of course, cyberbullying doesn't consist of only blackmail or hacking into private systems to make an entity unstable, it also consists of crimes like cyberstalking, unparliamentary comments and discrimination in social media, copyright crimes, etc. Now how to avoid these types of crimes. Common sense reasoning in cyberbullying is basically figuring out which content is bad or good based on the rules set by the society or oneself. Implementing this to tackle cyberbullying can be done through machine learning and hence the reason for AI to be best solution to stop cyberbullying.[6] Many economic and environmental factors pressure building operators and owners to adopt 'IoT' into their buildings. This has led to increased cost savings, power efficiency and process visibility. But integration of these technologies poses various design and cyber security challenges. We need to absolutely consider these challenges because failure can result in mass deaths and leakage of information. The various technologies that are used are CCTV motion

detection, RFID tokens and environment monitoring systems. In addition to this, research is being done on sensors which use artificial intelligence. They gather behavioral data, which can precisely predict why or how the society might react to a particular situation. Advancement in this field of work can lead to the development of a system that can learn to recognize patterns to respond to threats immediately.[7] Security used in communication is the main reason for cyber-attacks rather than hardware failure. Research is going on in identifying the failure in the system. This is where AI comes in. Machine learning helps AI to learn from data and access time. The human brain is not capable of detecting varieties of variables at the same time. It faces difficulty with coping up with environments which different while decision making. That's why AI is used. One of the most important processes in network security is intrusion detection. So, we create an intrusion detection system. It actually works in a very interesting way. It monitors the network by checking whether the system is overloaded. If it's the case, the AI will collect all the connected systems' information. This is very efficient because system's execution will not be affected during the process.[8] The safety of AI can be improved by the ideas of cybersecurity experts. But any security system has a chance of failure which is inevitable. And when a super intelligent system fails, the consequences will be catastrophic. There has been a lot of incidents at which AI has failed. Deadly accidents have been caused in the earlier days of AI. The failures can be classified into mistakes caused during the performance and learning phase. The incidents were such as, a software learned to cheat instead of making discoveries, a nuclear attack warning system falsely alerted that a nuclear attack is taking place, etc., In addition to AI failing to protect a network, AI itself could be a threat to the network. We haven't got lots of ways to analyze, monitor and visualize the performance these security systems. Because we don't even know what the software will do after it runs.[9] One of the fields that could be the most benefitted by Artificial Intelligence is cyber security. Since, when the first DoS attack happened in 1988, there has been a large number of cyber-attacks. Security systems should constantly adjust to the changing environment. As a lot of flexibility and adaptability is needed, humans alone can't find and fight these threats. And when AI was discovered, it was thought that it could break all these boundaries. There is a large amount of data, and the data was transferred at high speeds. The heterogeneity of the sources of data also made it difficult for humans to gather cyber intelligence. These issues could be easily mitigated through Artificial Intelligence. Neural networks that could learn and process data exactly like the human brain uses past network attacks and activities to prevent future exploits. But any system has drawbacks. AI has drawbacks such as data privacy, lack of regulations and ethical concerns.[10] The solutions for preventing cyber security incidents is becoming more and more complex. So, it's hard to develop a code that can fight these attacks. So, the code needed can only be developed by a being which can process data faster than a human being. And that's where AI comes in. But as many institutes have predicted, rapid development of computing intelligence will occur soon. They fear that a 'Singularity' might occur i.e., AI becoming smarter than humans. But before all that AI's cyber capabilities should not become accessible by offenders (hackers, phishers) as the tech might help them more in breaking into user accounts and leaking sensitive information.

Findings

The development of artificial intelligence is substantially increasing as the day goes along with it we have the different types of malware are also improving. So, from this we see as the technology increase in defending our systems there will also be problems arising in it too. We found different

types of problems are improving like DDos, forced authentication, intrusion algorithms and much more. But the ways to tackle such problems are also found like brute force management, application of computational intelligence which has a sub category of neural networks, artificial immune systems, fuzzy logics to create confusion to malware and of course machine learning as well. Several technologies in IOT, RFID, CCTV are also used in our day to day life and providing security to these is one of main implementation of AI. Cyberbullying is also seen to be decreasing due to this and many theories like common sense reasoning is also used. Many industrial, private sectors are affected by network intrusion and till now the only reputed solution to solve all these problems is the implementation of AI defense.

Recommendations and Conclusion

The number of cybercrimes are increasing very rapidly. Many companies have provided their products and support to stop all these. To find a prominent end to this impossible. The human mind will never be able to comprehend all types of possible breaches in a network system but an AI can. On the contrary AI itself can be a threat to network and its related entities too. The laws in cyber crime are not that helpful as if you don't know who to blame then you can't keep anyone responsible to the damage caused. Hence there should be a governing body always looking through the wide network, the internet, to subdue these kinds of problems. Moreover, the governing body can find people who are indulged in such crimes and then correct their morals and use them as resources to fight cybercrimes with the continuous support of artificial intelligence.

References

Anitha, A., Paul, G., & Kumari, S. (2016). A Cyber defence using Artificial Intelligence. International Journal of Pharmacy and Technology, 8(4).

Atkinson, D. J. (2015, March).Emerging cyber-security issues of autonomy and the psychopathology of intelligent machines. In Foundations of Autonomy and Its (Cyber) Threats: From Individuals to Interdependence: Papers from the 2015 AAAI Spring Symposium, Palo Alto, CA. http://www. aaai. org/ocs/index. php/SSS/SSS15/paper/viewFile/10219/10049

Dasgupta, D. (2006, October). Computational intelligence in cyber security. In Computational Intelligence for Homeland Security and Personal Safety, Proceedings of the 2006 IEEE International Conference on (pp. 2-3). IEEE.

Dinakar, K., Jones, B., Havasi, C., Lieberman, H., & Picard, R. (2012). Common sense reasoning for detection, prevention, and mitigation of cyberbullying. ACM Transactions on Interactive Intelligent Systems (TiiS), 2(3), 18.

Mittu, R., & Lawless, W. (2015, March). Human factors in cybersecurity and the role for ai. In Foundations of Autonomy and Its (Cyber) Threats: From Individual to Interdependence, AAAI Spring Symposium Series (pp. 39-43).

Mylrea, M., &Gourisetti, S. N. G. (2017). Cybersecurity and Optimization in Smart "Autonomous" Buildings. In Autonomy and Artificial Intelligence: A Threat or Savior? (pp. 263-294). Springer, Cham.

Patil, P. (2016). Artificial intelligence in cybersecurity. International Journal of Research in Computer Applications and Robotics, 4(5), 1-5.

Rajbanshi, A., Bhimrajka, S., & Raina, C. K. (2017). Artificial Intelligence in Cyber Security

Wirkuttis, N., & Klein, H. (2017). Artificial Intelligence in Cybersecurity. Cyber Intelligence, and Security Journal, 1, 21-3.

Yampolskiy, R. V., & Spellchecker, M. S. (2016). artificial intelligence safety and cybersecurity: a timeline of AI failures. arXiv preprint arXiv:1610.07997.