Role of Artificial Intelligence in Cyber Security: A Useful Overview

Vaishnavi Shukla, Amit Kumar Tyagi

VIT Chennai

Vshukla1622@gmail.com, amitkrtyagi025@gmail.com

Abstract. Cyber security has been an emerging concern of individuals and organizations all over the globe. Although the increasing dependance of the world on the internet proves to be an advancement of technology but it also happens to be a threat to important and private information, monetary fraud leading to huge losses for organizations, and many other issues. In this day and age, cyber security has become a great necessity and great efforts have been made to enhance it for several years. Artificial intelligence has emerged to be of immense importance over the past decade and is expected to bear great fruit in the coming time. It is to no surprise that organizations are depending on AI driven technologies to protect their data. AI along with concepts of Machine Learning and Deep Learning is being used to develop new and improved means to help in the cyber security domain. These intelligent systems will lead to an intelligent and automated security system giving it an edge from the conventional security systems. The scope of this paper covers a few Artificial intelligence concepts which have been used in the past to ensure security, a few ideas which have been discussed for future implementation, threats of using AI, etc.

keywords: artificial intelligence, cybersecurity, machine learning, supervised learning

1.Introduction

1.1History of Artificial Intelligence

We owe the seeding of the idea of Artificial Intelligence to **Alan Turing** who first gave a mathematical approach and idea in his paper **Computing Machinery and Intelligence** in 1950. However, computers in 1949 could not store command but only execute, hence there was a need to fundamentally change computers. Also, computing was extremely expensive. These were the two major factors holding back Turing from following his pursuit.

It was then a program designed by **Allen Newell, Cliff Shaw, and Herbert Simon** called **Logic Theorist** which mimicked the problem-solving skills of a human which brought the idea of Artificial Intelligence closer to reality. This program is also considered to be one of the first programs of AI.

Even though with time the understanding of Artificial Intelligence grew the main issue was still not solved, the computers were not advanced enough to carry out intelligent programs.

However, with time, the computational power of machines improved along with their storing capacity to a point where Moore's law had caught up.

Moore's law states that the number of transistors on a microchip double every two years and the cost of computer reduces by half.

By the 2000s AI had achieved many of its goals and this was the starting of an era where Artificial Intelligence became a field everyone had their eyes on.

1.2 History of Cyber Security

During a research project ARPANET, a program called Creeper was made which moved across ARPANET's network and left a message "I'm the creeper, catch me if you can" wherever it went.

Ray Tomlinson-the inventor of email, made a program called Reaper which tracked and deleted Creeper. Reaper was the first instance of an Antivirus.

By 1990s a lot of work on the antivirus part was being done and by 1992, the first antivirus program appeared

Soon as the world started coming online, virus attacks as well antivirus started getting more and more well known.

Soon antivirus like McAfee came to the market, still being widely used.

By 2000s more antivirus came into picture and now we can see an antivirus on almost every device.

2. CyberSecurity and AI

2.1 Principles of Cyber Security

There are certain principles followed to ensure cyber security. They are as follows:

1. Confidentiality: the information should be secure and shared with authorized personnel only and no unauthorized parties should have access to the information
2. Integrity: cybersecurity to ensure that the information should be accurate, consistent and free from any modification from unauthorized organization to maintain the integrity of the information
3. Availability: the cybersecurity efforts should not hinder the access of information by the authorized parties and also provide redundancy access in case of an outrage.

These are the basic principles of cybersecurity and we shall now look at the need of Artificial Intelligence in the field of cybersecurity.

2.2 AI in Cyber Space

Increase in the cybercrime activities initially posed a threat as there were not enough cybercrime professionals to handle the increasing threats. However soon after AI came to the rescue, making machines independent enough to handle these threats on their own.

Whenever a cyber activity takes place, AI plays its role in the following 3 stages-

Data is collected from the user-it is processed by the system being managed by security vendor-the detection system flags the malicious activities and may or may not generate an action in response.

With newly emerging concepts like IoT (Internet of Things) it has come to the companies' notice that the cyber dependency of the users is going to serve as a platform for attackers to play their part.

There are two ways to reduce cyber-attacks in this case-slowing down the attackers, speeding up the defenders.

For speeding up defenders, AI has proven to be an excellent solution. Traditional security had to spend a lot of time manually processing the alerts and figuring out if they are harmful or not. With the growth in AI sector, most of these tasks are being done by the machines independently and hence speeding up the defense.

In the past the focus was first on categorizing the malware but nowadays companies are opting for models that don't look for individual pieces of malware; rather they look for the behavior exhibited by the attackers. This behavior is then analyzed and the models are trained as per these instances. Hence it has become more common to opt for Machine Learning based threat detection systems. With time these models become more durable and eventually have the potential of detecting zero-day attacks.

2.3 Increasing Cyber Threat

- Internet of Things is a fast-growing domain and we can see the ever-growing market of it. However, since it is dependent on the data of the user which is processed by the internet, any leak of this data can lead to great risk. The main issue in this aspect is the lack of authentication and encryption of the data.
- Newly emerging payment systems like bit coin and Ethereum have taken over the public eye. It is based on the concept of block chain. Block chain seems to have more applications in the coming years in the field of medical record management, decentralized access control and identity managements.
- Large connection of devices being infected by the malware is called Botnet. This is one of the most threatening attacks as the increasing use of Iot along with devices belonging to the same server, or connected to the same internet network are under threat. If the attackers get through and reach any one of these devices, it is not that great of a challenge to reach the other devices and if they happen to be lucky, with only one device's

access they might be able to get a great deal of information and misuse it.

- Studies have shown that android devices are one of the most targeted devices for malware attack. Out of 14 applications made for malware detection, 8 were for android devices.

2.4 Network Intrusion

When an unauthorized party enters a network without the permission of the network owner, we refer to it as Network Intrusion.

Network Intrusion takes place in the following stages:

1. The information regarding the target is collected and analyzed for the weak and strong points. The information could be anything from email address to open-source details and specifically any detail regarding the network is looked upon with great attention.
2. In the exploitation stage, the attackers patiently keep visiting the websites frequently visited by the victim. The attackers are usually slow and take their steps with utmost care to avoid getting caught.
3. The intruders then steadily increase their activities and start making their way into scripts and keys under the network.
4. After this there comes the main stage of installing the malware into the network starting with less harmful ones and making their way onto installing more powerful malwares.
5. Slowly the intruders gain complete control over the network and can now access any information they wish to. The intruders gather all the necessary information and then leave the network.
6. Some of the intruders are also careful enough to erase their traces in order to prevent getting caught.

Different attacks of Network Intrusion include Trojans, Worms, Traffic Flooding etc.

A Network Intrusion Detection System analyzes incoming and outgoing packets to recognize patterns which may cause threat disguised as normal packets. For example, it can be installed on the subnet where firewalls are so that the NIDS can identify any attackers trying to break through the firewall. When a threat is discovered, the NIDS alerts the administrator which then overlooks the security of the network.

Machine learning approach

Machine learning to a great extent is dependent on the data sets on which it is trained.

The main task of NIDS boils down to classifying the packets into normal or abnormal. One of the most robust and functional methods which can be applied to perform this task is a supervised learning machine learning model.

For a classification of normal or abnormal, or in other manner into 0(for normal) and 1(for abnormal or vice versa), we can opt for a binary classification model.

The model is first given a huge dataset having instances of real modern normal activities and attack behavior. This data is then used to perform feature selection, where only feature correlated with label variable are selected. To perform this task, we can use any of the popular supervised learning algorithms. Here we have discussed three of them:

Logistic regression:

In this approach, the main prediction function comes out to be

$y' = mx + c$

Where,

y': predicted output

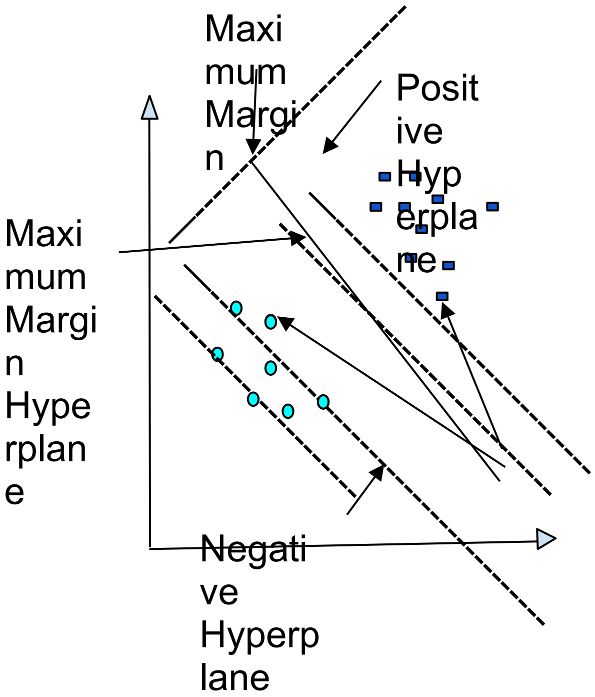
m: slope of the line

c: intercept

There are a number of methods and formulae which are used to calculate the value of m and c. These values are calculated after being trained by huge amounts of data. Once the best possible values of m and c are available, we then go ahead and use this function to test our data.

Support vector machine:

The basic idea of support vector machine is to draw a line or plane, or a hyperplane, which is farthest away from both the datasets on a graph.



In the picture above we can see the green and blue data points, these belong to two different classes. The maximum margin hyperplane is a plane which is farthest away from the nearest datapoint of both classes.

We can further apply optimization techniques such as Minibatch gradient descent or Stochastic gradient descent and get the best vector to classify our dataset.

When a new dataset is introduced or tested, depending on the location of it on the graph, it is classified into either of the two classes.

Decision Tree:

A decision tree, as suggested uses a tree data structure and every internal node is a binary condition. It is drawn upside down with the root nodes at the top. It splits into two branches that meet another node; the nodes are yes-no branches. The nodes which do not split into branches are knows as the decision nodes. These nodes decide which class the data belongs into.

All of these classification algorithms are used to classify our packets and for the detected abnormal packets, the system alerts the administrators who in turn check whether the network has been intruded or not and take the necessary actions.

2.5 Malware Detection

In the simplest terms, malware is piece of code designed to harm computer networks and misuse the data in them. The trick however is that the malwares only cause harm once they have been installed or implanted completely.

Malware detection is used to detect whether a certain program happens to be harmful or not. As discussed, since malware detection is also an act of classification, machine learning happens to be a great solution.

The growth of Neural Networks is a great step forward in the AI world. One of the biggest issues that AI has to overcome is false positives. False positive refers to an error in binary classification where an outcome wrongly indicates that an event has occurred when it actually has not. Neural networks improved the accuracy of models and also helped overcome false positives.

An approach which is spoken of is Artificial Neural Network which is greatly used under the umbrella of deep learning. As discussed earlier, it is inspired from the neuron in the human brain and consists of multiple layers. The output of each layer is an input to the next layer. ANN is greatly used and is one of the best algorithms provided data is sufficiently provided. Although a bit more challenging to understand compared to the other algorithms, the output of ANNs is greatly appreciated in terms of accuracy and robustness of the algorithm itself.

For malware detection, we again analyze the lines of code and normal codes are passed whereas abnormal codes are detected and analyzed further either by the AI itself or by cyber security personnel.

On similar notes, AI has become one of the most important aspects of the cyber security domain in the past few years. Let us discuss a few benefits to understand what has caused this change.

3. Benefits and shortcomings

3.1 Benefits of using AI and ML based cybersecurity models

- It improves over time. The Machine Learning and Deep Learning algorithms study and analyze the behaviors of business organizations and clusters them. It then detects any deviation in behavior from the norm. With time, the data it analyzes, makes the algorithms better and more sensitive.
- With time attackers have adapted to new technologies as well. The traditional methods may not be able to notice certain threats but AI has the potential to identify certain threats which may go unnoticed otherwise.
- On a daily basis, huge amounts of data are exchanged between networks out of which some of the malicious activities might go unnoticed by cybersecurity personnel. AI is able to process huge amount of data and hence happens to be a better option.
- Analyzing and assessing the existing security measures through AI research can help in vulnerability management. AI helps you assess systems quicker than cybersecurity personnel, thereby increasing your problem-solving ability manifold. It identifies weak points in computer systems and business networks and helps businesses focus on important security tasks.
- An organization may have to deal with a phishing attack along with denial-of-service attack or ransomware all at once. In these cases, prioritizing the attacks becomes essential as negligence at one spot can cost you a lot. AI helps in prioritizing these attacks and handling them using minimum time.
- Although avoiding major threats is a challenging task but regular basic checks must also always be made to avoid small attacks. These attacks might be neglected by cybersecurity personnel. AI on the other hand takes care of duplicative cybersecurity processes for basic security threats and prevent them on a regular basis.
- It accelerates the detection and response time. AI does regular system checks and keeps the detection up to date. Along with this its response time to an identified threat also keeps severe data leak in check.
- AI ensures authentication every time a user logs into website. These websites can contain information that is sensitive to the user and hence authentication becomes an essential step before accessing any website. AI uses the help of facial recognition, CAPTCHA, fingerprint scanner and other means to carry out regular authentications.

3.2 Is AI always good?

We have seen the advantage of AI in the current space but we cannot turn a blind eye to the increasing threats being caused AI.

Newer attacks, different in nature from the once executed traditionally have been on the rise and these attacks are designed specifically to strike AI systems. AI researchers have agreed that AI has affected the cybersecurity landscape by- expanding existing threats, introducing new threats, altering the characteristics of cyber-attacks.

Existing threats

In the current time, the concepts of AI and ML have become widely available to the general public and the availability of codes is also wide. This has gathered a large number of people understanding the working of malwares.

The widening growth of cheaply available hardware and freely available software resources has resulted in an increase in number of attackers.

Introduction to new threats

The involvement of AI has not only accelerated the existing threats but also given birth to new methods of attacking.

One of the means have been termed as “Deepfake”. Using Deep Learning algorithms, machines have become capable of forging faces, voices, texts and many more such things. Certain algorithms are used where, on being fed thousands of images of two people, the system is able to break down their facial features on the basis of similarities and difference. This is used to beat facial recognition systems.

On a similar note, voices too are forged. Some of these algorithms require less than four seconds of training audio to recreate human voices. One of the famous attacks on this track is when an AI based software imitated a chief executive's voice and requested a transfer of €220,000. The CEO thought that the chief executive was the one talking and transferred the amount from the German parent company to the Hungarian subsidiary.

Text manipulation is another dangerous threat. Although text manipulation is easy to beat but it can be used in various ways to waver the public opinion and can be used widely in political battles.

While internet and email scams have been around for decades, deepfakes have increased the tendency of these emails appearing to be real, trapping more and more victims.

Changes in typical characteristics

AI based cybersecurity is solely based on analyzing the lines of codes. The cyber attackers have thus opted for writing their codes in a way which exploits the AI vulnerabilities and makes the AI unable to function at its full potential.

Most of the cyberattacks are targeted towards stealing information or disrupting the working of a system. Newer attacks tend to go forth with a long-term plan. They wait and study the working of the system and as time passes, begin to interfere with its working and steal the required information.

This can be done in many ways- giving flawed data to the models. Stained data set will interfere with the training of the models and then hamper with the working.

Tampering the categorization models can be fatal to most of the ML models. Since the very basis of the ML models depends on the training data provided to it. If the algorithm itself is hampered, there is a chance that the categorization will prove to be ineffective and the cyber attackers will end up being successful in breaking through the AI system.

Ethical challenges

AI systems are effective in self-healing and self-testing. However, without any human intervention, the machine can very well walk into a path of destruction. The independence of AI system does reduce human efforts greatly but it also poses a threat to the ethical undertakings of a task which can be negatively impacted without any human supervision.

The growing dependance of organizations on AI for cyber security could ultimately lead to vast deskilling of experts and might eventually lead to a period when humans will be incapable of stopping the interaction between two AIs.

3.3 What the future holds

Back in the days, cybercriminals were people with good coding knowledge but that no longer is the case. Malware is sold around and bought by people making them capable of easily breaking into systems.

With automation also becoming one of the most popular fields of interest, malwares have also started to become automated. In the future, malwares will no longer be monitored by people. Malwares and the security models will fight a battle of their own. Although this might sound like a mere fight between two programmed systems, the data at stake can cause huge losses to organizations and individuals.

As time goes by, cybercriminals have increased in number, especially considering the COVID phase where most of the industries shifted to an online mode of communication. But were the cybersecurity cells enough in number to counter it? The biggest issue in the coming future can be the shortage of enough skilled cybersecurity specialists which will help in maintaining the security of such huge amounts of data.

It is no surprise that most of the organizations are invested in stronger and better cybersecurity systems. The importance of these defense mechanisms is increasing day by day and will continue to grow in the coming future with Industry 4.0 spreading further and AI entering more and more industries.

While the threat of AI on jobs is a widely debated topic, the cybersecurity employees have a bit of time before they start worrying about it. Although it will reduces the jobs in places where manual segregation of incoming data is required, it will create more jobs in area where maintenance of the AI is required.

Infact, it has been found that the industry is lacking of expertise. This does create more job opportunities but it requires highly skilled individuals, hence there is a need to train more individuals in this field to fill the gap that has been created through the years.

4. Conclusion

AI has been in the market for a few years and its applications have been growing continuously. This has resulted in a huge change in industries. Every organization wishes to switch to online mode of communication and have a more tech friendly representation for themselves. While this approach does seem the most functional, cost effective and attractive, it does provide a huge opportunity for the attackers to play their part.

The general public has also become more aware of the threat regarding cybersecurity and has become more cautious in terms of sharing their information online. While there have been efforts made by cybersecurity and Artificial Intelligence specialists to reduce the criminal activities going around, a huge difference will be made if the public itself is taught about safe sharing of data and how to avoid websites and emails appearing to be malicious.

Most of the people have antivirus and other programs installed into their systems to avoid getting into the hands of malicious attackers.

AI will improve with time and its use will grow further into more fields. As discussed earlier, although it will provide better security features, it will also provide a wider area of attack for cybercriminals.

5. Common Terms used

Let us first start by discussing a few terms under the umbrella of Artificial Intelligence for better understanding of this paper. Giving human like intelligence to machines has always been a topic of great interest among scientist as well as common public and with the current wave of technological advancement, machines have proved to be more and more intelligent. This is nothing but an instance of Artificial Intelligence.

The Organization for Economic Co-operation and Development (OECD) defines an AI system as a "*machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.*"

Machine Learning is a branch of Artificial Intelligence which focus on using data and applying algorithms to make predictions and classify data. Machine Learning broadly has three types of classification algorithms, supervised learning, unsupervised learning and reinforcement learning.

Supervised learning has data which already has a correct answer whereas in unsupervised learning, the algorithms cluster the data without any prior knowledge. Reinforcement learning uses a penalty system where the algorithm rewards itself for a correct classification and gives a penalty for incorrect one.

One of the most interesting subsets of Machine Learning is Neural Network. It is inspired from the neural networks present in the human and later led to Artificial Neural Networks (ANNs) which are used in Deep Learning.

Neural Networks rely on data to learn and improve their accuracy but once the algorithm is finely tuned, it can be used to classify data at a very high speed.

Cyber security is the act of protecting computers, mobile devices, servers, networks and data from malicious attacks.

Cyber threat is on an increase specially threat to medical and financial data is severe and hence there is a need to tighten the security surrounding these fields.

One of the most common ways of cyber-attack is malware. Malware is a malicious software which is meant for damaging a user's device and is often installed into devices by unsolicited emails

Firewall is a network security device which is used to monitor the incoming and outgoing packets in a network. It follows a set of security rules, based on which it blocks the packets it finds suspicious.

There are several approached in the domain of AI which can be used for our purpose such as a knowledge-based approach which uses several IF-ELSE conditional statements or a pattern-based approach where the data is fed into the algorithms and a pattern is noticed to carry out the algorithms.

References

1] See OECD (2019), AI Policy Observatory, 22 May.

2] OECD (2019a), “Artificial Intelligence in Society”, OECD Publishing, Paris (https://doi.org/10.1787/eedfee77-en)

3] B. Buchanan and T. Miller (2017), “Machine Learning for Policymakers, What It Is and Why It Matters”, Belfer Center for Science and International Affairs Harvard Kennedy School, June.

4] M.Drolet (2020), “The Evolving Threat Landscape: Five Trends to Expect in 2020 and Beyond”, Forbes Technology Council; Orange Business Service (2020), “2020 Security Landscape”

5] MacAfee (2020), “McAfee Labs Threats Report”, November.

6] Fortinet (2020), Enterprises Must Adapt to Address Telework Security Challenges: 2020 Remote Workforce Cybersecurity Report”, August

7] Palo Alto Network contribution to the fourth meeting of the CEPS Task Force.

8] Vectra’s contribution to the kick-off meeting of the CEPS Task Force.

9] MITRE ATT&CK

10] M. Brundage et al. (2018), “The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation”, Malicious AI Report, February, p. 18.

11] “artificial intelligence relies on algorithms that are easily replicable and therefore facilitate proliferation. While developing the algorithm takes some time, once it is operational, it can be very quickly and easily copied and replicated as algorithms are lines of code”, J.-M. Rickli (2018), “The impact of autonomy and artificial intelligence on strategic stability”, UN Special, July-August, pp. 32-33.

12] I. Sample (2020), “What are deepfakes and how can you spot them” The Guardian, 13 January

13] K. Vyas (2019), “Generative Adversarial Networks: The Tech Behind DeepFake and FaceApp”, Interesting Engineering, 12 August .

14] K. Hao and P. Howell O'Neill (2020), “The hack that could make face recognition think someone else is you”, MIT Technology Review, 5 August.

15] R. Diresta (2020), “AI-Generated Text Is the Scariest Deepfake of All”, Wired, 31 July.

16] B. Paris and J. Donovan (2019), “DeepFakes and Cheap Fakes: The Manipulation of Audio and Visual Evidence”, Data and Society, September, p. 41

17] A. Ridgway (2021), “Deepfakes: the fight against this dangerous use of AI”, Science Focus, 12 November.

18] R. Irioni (2018), “Breaking CAPTCHA using Machine Learning in 0,05 Seconds”, Medium, 19 December and E. Zouave et al. (2000), “Artificial Intelligence Cyberattacks”, FOI, p. 24.

19] J.-M. Rickli (2018), The impact of autonomy and artificial intelligence on strategic stability, UN Special, July-August, pp. 32-33.

20] (ISC)2 (2019), “Strategies for Building and Growing Strong Cybersecurity Teams”, (ISC)2 Cybersecurity Workforce Study.

21] S. Morgan (2015), “Cybersecurity job market to suffer severe workforce shortage”, CSO Online, 28 July.

22] C. Barlow (2015), “Perspective: Artificial intelligence makes cybersecurity the ideal field for ‘new collar’ jobs”, Duke Political Science Blog

23] M. Dsouza (2018), “How will AI impact job roles in Cybersecurity”, Packt, 25 September.

24] Chatzigiannakis, V., Androulidakis, G., & Maglaris, B. (2004). A Distributed Intrusion Detection Prototype Using Security Agents. In Proceedings of Workshop of the HP Open View University Association. University of Evry.

25] Johnson, J. (2014). Remarks by Secretary of Homeland Security Jeh Johnson at the White House Cybersecurity Framework Event.

26] Kivimaa, J., Ojamaa, A., & Tyugu, E. (2008). Pareto-Optimal state of affairs Analysis for the selection of Security Measures. Proceedings of Military communications conference, MILCOM 2008.

27] Kivimaa, J., Ojamaa, A., & Tyugu, E. (2009). Graded Security accomplished System. In Lecture Notes in engineering (Vol. 5508, pp. 279–286). Springer.