THE EVOLVING ROLE OF AI/ML INCYBER SECURITY

Abstract

The protection of data or systems from malicious threats or attacks is known as cyber security. These attacks can take place by changing or deleting anyone's personal information or data. This paper discusses about the cyber security and its current scenario today and how with the help of Artificial Intelligence and Machine Learning the cyber security industry can be secured, various algorithms of Machine Learning are also been dis- cussed with the help of which any anomalies can be detected in prior to their occurrence. With the help of AI thethreats which have already took place, the system keeps a record of their happening and any threat similar to the preceding threat can be acknowledged easily and how the future of cyber security can completely be retransformed with the implementation of AI and ML. The objective of the paper is to find out about the current scenario of cyber security and how attacks are being promulgated and how to control them by using various tools and impending risk management, to find out what is artificial intelligence and machine learning and how are they changing the shape of cyber security industry, and how with the use of various devices and with the help of algorithm of machine learning cyber-attacks can be prevented to a greater extent as the algorithms are able to find out whether the data is compiled of threat or is secured and how with the help of the databases the al- ready occurred attacks can be used as a vital information to tackle the forthcoming attacks.

Keywords: Machine Learning; cyber-attacks; cyber security; Expert System

Authors

Rana Majumdar
Sister Nivedita University
West Bengal, India.

Pratik Bhattacharjee
Sister Nivedita University
West Bengal, India.

Anirban Mitra
Sister Nivedita University
West Bengal, India.

Soma Hazra
Sister Nivedita University
West Bengal, India.

I. INTRODUCTION

Cyber security is the preservation of systems that are connected to the internet on a big platform such as hard- ware, software, and other important information from cyber-attacks. The individuals and other ventures often do these practices to be safe against unauthorized access to data centers and different computerized systems. The main target of carrying out cyber security is to cater a better security masquerade for various computer systems, mobile devices, servers, networks, and the data gathered on those gears from cyber assailants with malicious desire. Cyber- attacks can be performed by accessing, deleting, or coercing an institution's or individuals private data, making cyber security a very important task. Cyber security is a constantly developing area, with the advancement of technologies that agape up new entrance for cyber-attacks. Moreover, only important security ruptures are the ones that often get promulgated, small institutions or organizations however must worry themselves with security ruptures, as they may also be targeted for viruses and phishing. Therefore, to save organizations, workers and other users, organizations should practice cyber security tools, training, risk management impends and constantly update systems as new technologies change and come up. Cyber Security composes of technology and methods particularly made to save PCs, laptops, networks, various kinds of applications, data from incursion, and illegally getting the right to access, alter or destroy the information or data. A Cyber Security design consists of community safety systems and host (PC) protection systems. Each of which has at minimum a firewall, an antivirus program, and imposition detection instrument. Scientists in the recent times are considering PC engineering statistics protection and cyber security as their mission. [1]

Artificial intelligence is basically the science of making computers, robots to think and act intelligently like humans and without their intervention. The primarily goals of AI are to make expert systems which include intelligent behavior, able to learn and demonstrate and advise its users. Other task of AI includes enforcing human intelligence in tools and machines so that the systems have the ability to understand, assume, grasp and act like humans. Artificial intelligence has been leading in several fields like natural language processing, expert systems, vision systems, speech recognition, intelligent robots, etc. [2]

Machine Learning is a part of Artificial Intelligence that enables the systems to naturally learn and enhance from the previous experiences without the help of any programming. Machine learning priory targets on the making of computer programs that can use the data and make use for their own. Machine learning basically constitutes of the observation of data, prior experiences so that better decisions can be made in the future. Various algorithms are been used in this process so that the computers might learn without any mediation of humans and make actions appropriately. The text is treated as keyword by the algorithms of machine learning, and the system makes it able for the humans to understand the text meaning.[3]

II. ROLE OF AI AND ML IN CYBER SECURITY

Artificial intelligence(AI) and machine learning(ML) are being broadcasted nowadays to help in various industries by solving a wide range of problems, like reducing the street traffic, enhancing the platform of online shopping, helping humans in day to day life with the help of voice assistants and many more. AI and ML are helping out in cyber security industry

as well; however it is advised to be careful of the advertising around AI and ML. If "Artificial Intelligence" is searched on Google, it gives around a million of results. But AI and ML nevertheless are really going to solve out all problems in cyber security. The organizations really need to point out the difference between what is actually real and what is being advertised when it comes out to AI and ML in cyber security. Basically, the primarily point need to be considered by organizations and enterprises is that AI/ML cannot tell us why something happened, to know about 'why' is a role of cyber security.

There are new security technologies that are using Artificial Intelligence solutions to find out unusual activity on the network. To identify similarities and discrepancy in a data set AI uses machine learning and report any aberration if detected. Machine learning is also a part of Artificial Intelligence that can stimulate to perceive patterns in data and forecast effects on past results and information. If we talk about most of the AI systems, they use machine learning technology that duplicate human functioning in order to give results. An article was published in Forbes with the title 'Separating Fact From Fiction: The Role of Artificial Intelligence in Cyber security', Machine Learning was coalesced with application isolation, avert the drawback of malware execution, isolation stamp out the breach, confirms that no data is arbitrate and that malware does not go paralleled onto the network. Cyber-attacks are also constantly changing in terms of speed. We humans are unable to identify the anomalies at the same speed at which attacks occur [4].

Artificial Intelligence can appraise a big amount of data produced on a network to detect what does not appertain there. If there is strong input of data, Artificial Intelligence can work more properly, therefore organizations or institutions can begin to bust their log data and centralize into a one common data vault thereby the vast set of AI-enabled tools and data can become useful. All aspects of networks should also be completely visible which consists of network communication that is done internally, server logs, etc.

Security professional nowadays are planning to use anticipating analytics to find out new ways to tackle with cyber threats. This can be done or enabled with the help of AI, machine learning can be used in anti-malware, doing dynamic risk analysis and identifying anomaly. If there is any noise or unwanted data AI techniques can be used to remove them, and ease the security experts to get to know about the cyber surroundings for identification of any anomalies. Cyber courses of action or COAs can be started with automated techniques provided by AI that can benefit cyber security whenever cyber threats come out. It is now advised that this is the time to seriously envisage artificial intelligence for cyber security if any venture or an enterprise is to be protected against cyber threats.[5]

Artificial Intelligence is nowadays very valuable to the cyber security industry, it compromises of the algorithms of machine learning that are easily able to detect and reciprocate to the attacks as soon as they take place. The algorithms are capable of anticipating whether the data that is received is malicious or secured. The attacks that take place necessarily need not to be new, even such kinds of attacks have taken place to some-body else, elsewhere. Hence if the information about the attacks that have took place are stored into a database and provided to machine learning algorithms, the threats and attacks can be forbid even before they take place. Other approaches uses the method of identifying the aberration while the data is been processed, and then collecting every point from the data and then using a particular algorithm to track the deviations which can identify that whether there has been a hack an incursion. The algorithms used by 'neural network and deep

learning' can perceive features from every kind of things, whether it is texts or images on the internet and through these features it concludes whether the data is malignant or not. Such features are enabled by processing a lot of data in a real quick time. Neural networks are difficult for humans to understand and interpret, and these networks never make mistakes after processing their past data.

III. HOW CAN CYBER-ATTACKS BE PREVENTED BY AI AND MACHINE LEARNING

Artificial Intelligence and Machine Learning are playing a very important role in cyber security now, the landscape of cyber security would be very distinctive than it is right now. Effective solutions are being discovered like AI systems and deep learning algorithms that are already playing their part in helping cyber security professionals. Since the cyber threats are evolving on a very huge number and the attacks are becoming more difficult to tackle and are becoming boundless, traditional tools and methods can't be used to identify and stop them on time. Hence, machine learning provides the security solutions that are the upcoming big thing in cyber security. Such tools and solutions have the ability to learn and comply over time, and they can easily eradicate the well-known threats and can also recall and refine data from prior attacks, thereby can respond to the risks that can take place before they do any harm. Artificial intelligence has the ability to implement particular tasks on its own, and in this way it saves time and human error risk is also reduced. AI systems can respond to each threat in a very effective manner by not making any errors or mistakes as they examine threats according to a regulated playbook.

Security experts now are keener towards building a stronger defense against cyber-attacks before they even occur rather than spending more time on routine tasks with the help of AI systems on their side. There- fore it is now important to implement and use AI systems and machine learning to stay forward of cyber criminals. The new exemplar for automation in cyber security is AI and ML. To mollify threats with lesser number of resources AI and ML enable auguring analytics to take out statistical conjecture. Self- encrypting and self- healing drives are a part of applications for automated network security to secure data and applications. In the current scenario of data engulf, humans find it nearly impossible to study the logs that are created in billions from the current infrastructure segments. There are many existing systems in which AI is introduced and that are "Security Monitoring Solutions, SIEM, Intrusion Detection Systems, Cryptographic technologies and Video vigilance systems" and it can really provide a helping hand in remitting many of the problems and challenges to a much larger scope. If AI based technologies are embedded into these systems it will provide a better decision making and provide much more enhanced systems. There are some fields where components of AI are making a difference are:

1. Data Mining
2. Pattern Recognition
3. Fraud Detection
4. Analytics
5. Fuzzy Logic
6. Development of expert systems

The above mentioned few aspects of AI if used in cyber security can bring in a lot of advantage, and few are already in place working in the sector and there are a lot of contingencies yet to be discovered. Malware like Polymorphic virus can easily be detected quickly and meticulously by the antivirus systems and tools that are based on machine learning and it depends on their continuous learning abilities. The threats can be identified at an early point of time by such systems by their mode of detecting cautious files based on the "behavioral or structural analysis". The possibility of a malignant virus attack can be easily obstinate by analyzing and structuring down the DNA of each file. Another facet of security other than AI and ML which The Cisco Cyber security Specialist certification is worried about is compliance. Every institute or organization has to be compliant with various regulations and being non- compliant to any of the regulations can result to big fines. If the organization turns out to be non-compliant, GDPR Regulation can cost 20 million euros or 4% of annual turnover globally.

The compliance status is been kept on track by the business organization with the help of cognitive computing offered by AI and ML in order to shun any legal problems. Machines provided with intelligence are man-aging automated cyber-attacks totally in this fast moving world. Such skilled systems have the ability to study the DNA of the past attack models, and through their gained knowledge can make new attack models with a greater achievement rate and greater impact. As the attacks are increasing day by day it is the hour of demand where organizations setup globally, the government and defense bureaus should come up together to implement AI and other technologies associated with it into their cyber security platform.[6]

IV. APPLICATIONS OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

The incorporation of artificial intelligence in cyber security has reduced the amount of cyber threats that is currently being faced globally. With the help of AI and ML very large amount of data can be stored and such data can be accessed by systems in a very short span of time resulting the corporates to identify the threat quickly. Earlier AI and security were treated as separate articles but now they are collaborating to ease the work. Various fields in cyber security where AI techniques are been used are:

1. **Expert Systems:** The human mind cannot retrieve or store large amount of information, such is in the case with cyber security where huge number of threats occur on a daily basis and to remember or store the information about these attacks is not possible for a human brain, therefore expert systems being a very sophisticated part of Artificial Intelligence comes into play which is able to store large amount of similar data and therefore can be used with cyber security for storing the information about the preceding attacks so that the expertise can have a knowledge about the attack and respond to it accordingly. Expert system consists of a knowledge base, an inference engine, explanatory machine and a knowledge acquisition system. The knowledge base complies of the information that is loaded into it. Every time an event occurs, the knowledge base is provided with the information so that the information or the data set can be used in future for the similar event without any searching or human effort. The inference engine composes of the extra information being added to it in relation to the data provided to the knowledge base. Expert system consists of two steps, first being constructing an expert system and second being providing information or data to the knowledge base. This expert system plays an important role in Battling cyber-attacks by storing information

about the threats every time into the knowledge base and the inference engine and then tackling a similar threat which might occur later by the use of knowledge base. If the threat ought to be different then the expert systems make use of inference engine so that it can search for extra in- formation to handle the new threat. The inference engine is always updated and extra information is been added to it. The knowledge base in case of cyber-attacks primarily consists of the following parameter such as malicious IP address, known viruses and malware, end point usage stats, etc. while inference engine has the following components such as geographical location of IP address, connection attempts, login attempts andport communication, etc. Hence due to the ability of prerecording of information expert systems offered by AI plays a very important role in handling cyber-attacks.

2. **Neural Nets:** Neural nets are a part of deep learning which in turn a part of artificial intelligence is. A neural net basically consists of artificial neurons, these neurons have the ability to learn on their own without any external help and they do all this by training. They are able to perceive information from data in the same way the human neural net-work is able to. When neural nets are connected to cyber security they can easily find out whether a document or a file is malicious or dangerous for the system or not without any help of humans. Neural nets are strongly able to detect the malware with the help of machine learning techniques and they can also cover up the digs through which any organizations can be presented before any attack. [7]

3. **Email Monitoring:** Various cyber-attacks are being conducted through emails these days. Several organizations receive unusual emails on a large account which might contain malicious content. While it is not really impossible for the employees to find out about the malicious mail but checking out for millions of mail is kind of impossible. Therefore there are tremendous AI software's which with the help of natural language processing are able to detect any harmful or undesirable content by checking out the texts and identifying phrases or patterns which might be related to phishing. This software also comes with the anomaly detection feature which can find out if the sender or the receiver of the email is of any kind of threat. And these software's can easily run into the incoming and outgoing emails and can detect for any abnormal content and can immediately report to the security expertise. [8]

V. CYBER SECURITY MONITORING USING MACHINE LEARNING

Cyber machine learning is one of the major fundamental of cyber security. Artificial Intelligence and Ma- chine learning technologies are now more embedded into the newer technology products of cyber security. The AI software's are inculcated more into the data files of cyber security which in turn is yielding positive results for the organization. Analysts predict that the organizations and the ventures will hold onto ML into each and every class of cyber security commodity.

Now a research with the help of Machine Learning techniques is been done and the primarily goal of the following work is to find out the anomalies in a real actual time by designing a particular gadget or a tool that has the ability of reading methods or strategies, that may sermon the issue of identifying anomalies by having no need of the framework of network.

Approach: Training, affirmation and test sets are been conceived after gathering the data from UCI machine, after preprocessing. The data collected will be transformed to the different input compositions with the help of various used algorithms which is a step of preprocessing, and it results into the formation of matrix where item collected is a row and each column is a feature. The values that are put in the matrix will be regulated such that no feature can have much larger value than the others, following this could lead into biased results for particular algorithms. This regulation comprises of 'subtracting its mean and dividing by its standard deviation'. This procedure also consists of picking of feature, which means applicable featured are been picked for the particular problem. And when the selection process of feature is been done then an ML algorithm is applied to build a model, that uses training, affirmation, and test sets. And with the help of this model network status can be classified.

VI. METHODOLOGY

System architecture is designed which comprises of various modules. "Data Collection, Data Preprocessing, Model Creation and performance Measurement, and Network State Identification" area part of these modules. The Data Collection module defines the user to gather the data which can be analogous either to a non- anomalous network or an anomalous network or the case is anonymous. The time consumed during the collection of data, and which device or gadget is to be observed can be specified by the user by mentioning the IP address of the device. The values of the data get normalized and the data is divided into training, affirmation, and testing sets in the second module viz. Data Preprocessing. There are respectively two classification of the class algorithm, which are multi class and one class algorithm. The user must enumerate that with which class the data should be used, as, in a multi class algorithm there are both anomalous and non- anomalous data is used in all particular sets, whereas in a one class algorithm the anomalous data is used only in the testing set. A machine learning algorithm is been implemented to train, save, and test a model in the third module which is also known as 'Model Creation and Performance Measurement' using the gathered data. The user in the third module only must decide which data set matrix to be used along with the machine learning algorithm.[9]

VII. CONCLUSION

Implementing AI into cyber security can turn out to be very useful if we talk about the current scenario. The AI systems have a number of advantages that helps the cyber security experts for tackling the cyber threats and protecting the venture or an organization. The forthcoming AI algorithms make use of machine learning and continuously modify over time. It is said that the use of ML in the algorithms makes it really accessible or effortless to acknowledge the cyber security risks. If traditional protocols of cyber security are been applied then it becomes quite difficult to detect the malware or cyber-attacks of the new era, as they keep on emerging over time therefore more dynamic protocols are needed. The newer solutions that make the use of ML, utilizes the data from the preceding cyber- attacks to acknowledge the new. AI in cyber security is very commonly used for detecting simple threats and attacks, and given this the simple attacks also have the easier solutions, the problem is handled by the system on its own, thereby reducing a lot of time and effort for the technical employees. Moreover it is also said that the AI used in cyber security is decreasing the need to have a larger amount of staff as they rely on intelligent automation. AI systems

can also help in tackling the threats by classifying the attacks based on their threat level, and the system can decide which threat to first deal with. And with the help of this deep machine learning principles are been integrated into the systems which have tendency to acclimate over time which can give a dynamic leap over the cyber attackers. AI systems generally don't commit mistakes or make faults in doing their functions and each threat is been handled efficiently and properly as the threats are been standardized according to a procedure. Automation is used nowadays by the employees in order to solve most of the problems. Even cyber security experts are also using automation to use time more effectively and reinforce their work performance. Use of expert systems and neural networks can also be made into use in order to increase security in the expert systems. An AI system can also make use of the previous attack logs to anticipate the nature of the upcoming attacks and hence will be able to tackle it timely. It is believed that making use of such systems in the future can increase the security up to an extent that the attackers or hackers will find it very difficult to infringe. [10]

REFERENCES

[1] Cabaj, K., Kotulski, Z., Księżopolski, B. et al. Cybersecurity: trends, issues, and challenges. EURASIP J. onInfo. Security 2018, 10 (2018). https://doi.org/10.1186/s13635-018-0080-0
[2] Li, J.. "Cyber security meets artificial intelligence: a survey." Frontiers of Information Technology & Elec-tronic Engineering 19 (2019): 1462-1474.
[3] Xin Y, Kong L, Liu Z, Chen Y, Li Y, Zhu H, Gao M, Hou H, Wang C. Machine learning and deep learningmethods for cybersecurity. IEEE Access. 2018;6:35365–81.
[4] Bhatele, Kirti Raj,et al. "The Role of Artificial Intelligence in Cyber Security." Countering Cyber Attacksand Preserving the Integrity and Availability of Critical Systems, edited by S. Geetha and Asnath Victy Phamila, IGI Global, 2019, pp. 170-192.http://doi:10.4018/978-1-5225-8241-0.ch009
[5] Benoit Morel. 2011. Artificial intelligence and the future of cybersecurity. In Proceedings of the 4th ACM workshop on Security and artificial intelligence (AISec '11). Association for Computing Machinery, New York, NY, USA, 93–98. DOI:https://doi.org/10.1145/2046684.2046699
[6] 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.
[7] Sunil Bhutada, Preeti Bhutada, "Applications of AI in cybersecurity- Expert Systems and Neural nets" in In- ternational Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5, Issue 4, April 2018
[8] Petri Vähäkainu, Martti Lehto, "Artificial intelligence in the cyber security environment", in The 14th Inter- national Conference on Cyber Warfare and Security ICCWS2019, Stellenbosch, South Africa
[9] Y. Goyal and A. Sharma, "A Semantic Machine Learning Approach for Cyber Security Monitoring," 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2019, pp. 439-442, doi: 10.1109/ICCMC.2019.8819796.

