IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 5, May 2021

DOI: 10.17148/IARJSET.2021.8557

Implementing AI and ML for Cyber Security

Amit Umesh Patil[1]

Systems Engineer, Infosys, Chennai, India[1]

Abstract: In today's 21st century, cyber security is a bomb shell which is getting more attention as the increasing cyber-attacks and hacking processes has come up with very easy and unpredictable results. The aim is to provide significant view on what cyber security and artificial intelligence together is capable of. Cyber security and Artificial intelligence are inter-linked concepts. Artificial intelligence has been changing and evolving the whole world with newer surprises and excitement. It is yet an unrevealed paradise. AI provides smart and advanced capabilities in tackling challenging cyber security problems in the real world.

Keywords: Artificial intelligence, machine learning, super intelligence, cyber security implementations.

I. INTRODUCTION

"One single vulnerability is all an attacker needs."

Fig 1. AI and ML: The cyber security masters

Cyber security is a cat and mice game. A mouse has to find only one hole out of many holes to escape. But the cat has to keep eye on every hole and catch up the mice who is trying to fool the cat and escape. It deals with finding strengths and weakness and making sure that any kind of cyber-attack does not violate organizational security and protocols [1]. To mitigate any threats for organization, cyber-security can be combined with artificial intelligence technologies for advanced research, innovation and productivity assuring internal as well as organizational level security to maintain the cyber hygiene in real world environment.

II. CYBER SECURITY

What is Cyber security?

Cyber security is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation [2,3]. It consists of all the technologies and practices that keep computers, networks, and the electronic data they contain safe and secure, particularly involving the Internet. Like a fence around a house we put protections around our connectedness (phones, computer, network, devices and peripherals etc.).

Why Cyber security?

The cyber security is mainly based on a principle known as CIA triads. It forms the base for cyber security

DOI: 10.17148/IARJSET.2021.8557

professionals for performing work and research in the filled of security. Cyber security helps to provide some of major security concerns such as ::

i) Confidentiality ::
It helps to establish a strong privacy and confidentiality value which helps to ensure information remains private and restricted. Information disclosure to unauthorized people causes harm (financial loss). For example, personal information - SSN/PAN. We use a safe that can only be accessed by authorized people to protect our valuable information ensuring the right set of people having the right set of access.

ii) Integrity ::
Integrity involves safe guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. Integrity makes sure that data or action doesn't change once performed. Data is not altered. Using a wax seal on a hand written letter ensures that if unopened it is the original text. If broken, the letter is not trusted. We can do the same with signed emails for example. Integrity assures timely and highly reliable use and access to information.

iii) Availability ::
The information is useless if someone cannot access it. If there is no availability a user cannot access their data, website, email, or any of the important parts of their job. Data must be available to the users when they need it.

iv) Non-Repudiation ::
It can provide proof of origin of an object and can provide proof of receipt of an object. An entity can't deny that it received a data object or that it sent a data object. When we communicate electronically, we want assurance that someone cannot take action and pretend that they have not taken that action. It ensures that a sender can't deny having sent a particular message, or that a message recipient can't deny having received it.

v) Authorization ::
Authorization provides an approval for something that is granted to a system entity to use a system resource. It is a process by which a system determines if one resource can access or use another resource. We use information about a user to make sure the right user has the appropriate access. It is like a synonym for permission and privilege.

III. Artificial Intelligence

"There is no silver bullet solution with cyber security. A layered defence is the only viable defence."

Artificial intelligence is the one of the latest and most powerful technology invented by humans. Though humans are yet to discover the whole ocean full of knowledge and extremely unparalleled power it has. AI has capabilities to explore the undiscovered power of technology and with the help of machine learning, new superficial algorithms which helps the machine to have its own intelligence to take the decisions. There are ways in which artificial intelligence can be used with cyber security::

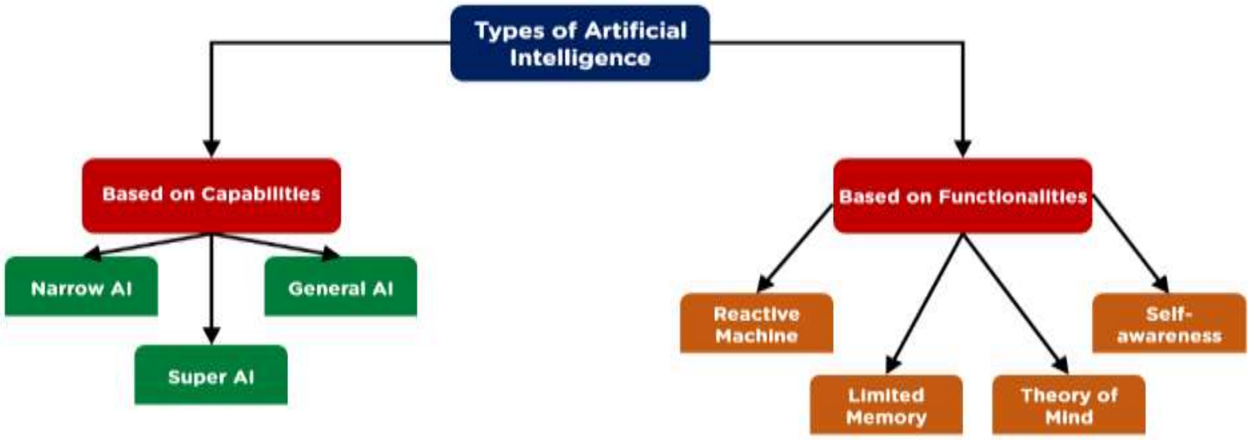

Fig 2. Types of artificial intelligence

DOI: 10.17148/IARJSET.2021.8557

Artificial intelligence is the intelligence developed for machines using various programs, algorithms and technologies leading to self-learning from past experience and developing ability to take probably most appropriate decisions and take necessary actions. [4]

Based on Capabilities::

i) Narrow/Weak AI::
Weak AI focuses on day-to-day work ease and productivity application development. It can be used to develop narrow spectrum tasks. It has some limitations in terms of its scalability.
EX. Apple Siri, Amazon Alexa, Bots, IBM Watson

ii) Super AI::
Super AI outperforms any sort of human intelligence and surpasses any task that can be done by humans. It can have its own self learning capabilities from past experiences as well as from spontaneously take probable decisions without any experience by its own adaptive algorithms and programming logics.
EX. Self-driving cars

iii) General/Strong AI::
Strong AI focuses on tasks that accomplish human intelligence into machine levels. It can perform task according to human intelligence and do things the way a human intelligence can do.
EX. Microsoft OpenAI, Super computers

Based on Functionalities::

i) Reactive Machine::
Reactive machine AI works on present data only. It can perform actions with supervised and predefined data and task. It does not develop its own intelligence depending on experience or anything , but performs specific tasks only.
EX. IBM Deep Blue

ii) Limited Memory::
Limited memory AI has a short term memory which works with past experience but for specific period of time. They work with real time collected data, do statistics and predict the output.
EX. Self-driving cars

iii) Theory of Mind::
Theory of mind AI is a still a concept in which machine understand human interactions, emotions, thought process and sentiments. It can also manipulate or alter human behaviour and feelings. It is still in its development stage and not fully acknowledged or experienced by the world.
EX. Sophia robot

iv) Self- awareness::
Self-awareness AI is one step ahead of theory of mind AI. It has hypothetical existence only. It can understand and perceive human conditions and behaviours, internal state without even letting humans to do anything. This AI can interpret emotions, beliefs on its own and perform the tasks independently.

IV. INTEGRATING AI AND ML WITH CYBER SECURITY

Artificial Intelligence and machine learning has been two buck wild technologies using which humans can achieve even the most difficult and unknown things. AI can be integrated with cyber security to help cyber security professional help with finding any loopholes and drawbacks in the system. AI can help to automate the monitoring and security operations process. It can predicate and spot out any DDoS, XSS or SQL and LDAP Injection attack. It can help to trigger out any brute force attack and restrict the attackers from accessing confidential data and information. Password hijacking, cookies and session hijacking, database vulnerabilities, uploading a scripted file and fetching system data, unauthorized access and privilege creep, all such attacks can be analysed and system can be trained with machine learning algorithms and implemented in such a way that these attacks can be restricted, and preventive measures can be taken with the help of AI and ML.

DOI: 10.17148/IARJSET.2021.8557

How AI and ML can be implemented for Cyber security::

i) IT Governance and Compliance::

AI and ML can help in providing governance and compliance for developing cyber security architecture in an organization. Various international standards and organizations like CISA, ENISA provide governance and guidelines for implementing cyber security. AI can help in enhancing those guidelines and providing strict regulations for the same. AI can help in identifying and detecting malicious activities and help protect and respond to those activities by implementing various machine learning and deep learning algorithms. HIPAA, FIPS, FISMA, NIST, PCC, etc. and many other international standards can be monitored in the system and any fraud or violation of such compliance can be triggered out by using ML.

ii) Privacy and risk management::

Any kind of financial, personal, professional and commercial as well as government and defence data can be managed and secured using strong ML algorithms and encryption technologies.

iii) Security Operations Centre (SOC)::

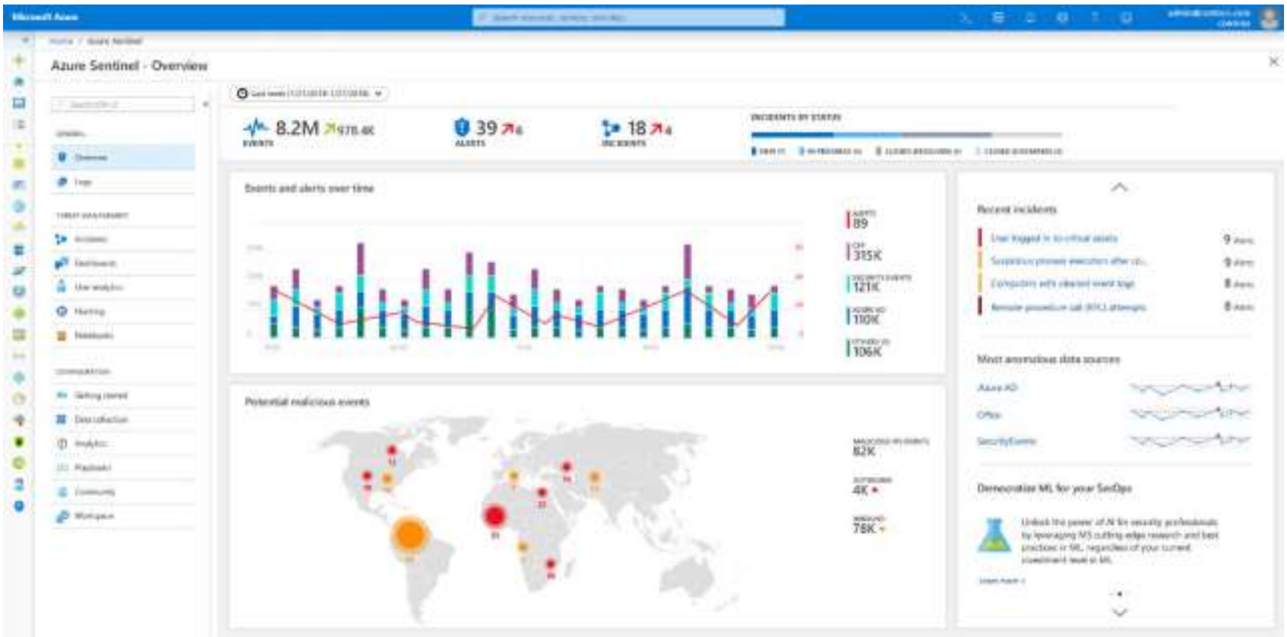
Microsoft Azure
Azure Sentinel - Overview
8.2M
EVENTS
39
ALERTS
18
INCIDENTS
INCIDENTS BY STATUS
Events and alerts over time
89
315K
121K
110K
106K
Potential malicious events
82K
4K
78K
Recent incidents
Most anomalous data sources
Azure AD
Office
SecurityEvents
Democratize ML for your SecOps

Fig 3. Microsoft's SIEM Tool : Azure Sentinel Dashboard

Continuous and aggressive Monitoring is a key factor for SOC operations [5]. Various monitoring security information and event management tools (SIEM) and security aspects can be enhanced using AI and ML. Multiple and adaptive dashboards can be designed and implemented using supervised and unsupervised machine learning algorithms [6]. Various filters and data logs can be provided so that any incident or malicious activity, unauthorized user activity, software, network and hardware integrity and management, overview of cyber activities can be monitored.

iv) Infrastructure Protection and management::

AI and ML can be used with cyber security for having a deep eye on all kinds of infrastructural assets.

- Application security
- Information security
- Network security
- Operational security

DOI: 10.17148/IARJSET.2021.8557

- Internet Security
- Hardware Security

v) Incident detection and management::

Incident can be detected and responded automatically by providing high level machine learning and neural network algorithms.

- Spam filters
- Fraud Detection
- Botnet Detection
- Unauthorized access prevention
- Hacking and Incident forecasting
- Network Intrusion Detection
- Credit scoring and ratings
- Brute force and scripting attack prevention

vi) Threat Intelligence::

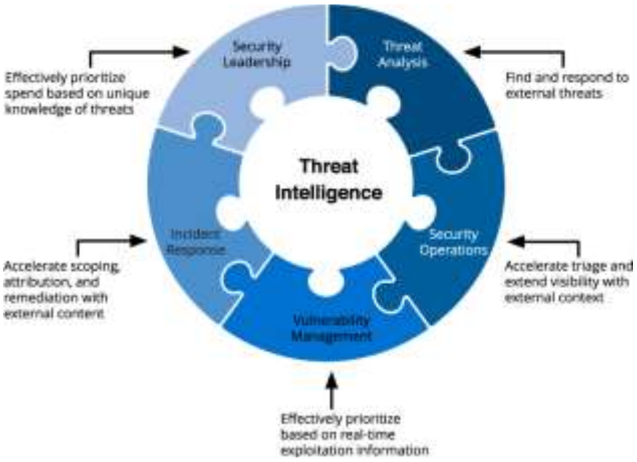
Security Leadership
Threat Analysis
Effectively prioritize spend based on unique knowledge of threats
Find and respond to external threats
Threat Intelligence
Incident Response
Security Operations
Accelerate scoping, attribution, and remediation with external content
Accelerate triage and extend visibility with external context
Vulnerability Management
Effectively prioritize based on real-time exploitation information

Fig 4. AI based Threat Intelligence

AI can be used in cyber security by automating the vulnerability discovery by implementing algorithms and statistics to the system [7]. Automation of social engineering attacks, sophisticated hacking, and service task implications in criminal offence and defence activities can be used to advance the existing cyber architecture using AI and ML [8].

vii) Cyber Training, Exercises and Hygiene::

This can be maintained by providing timely updates on latest malware, virus and ransom ware or attacks all across the world. ML can be implemented in such a way that system gets all the information about how to mitigate such newly discovered viruses and restrict them from getting affected to particular organization by developing automated patch management, antivirus and security response services.

Essential training, automated modules and practical datasets can be provided to the system as well as employees of the organization so that awareness and cyber space hygiene can be maintained [9].

V. CONCLUSION

AI and ML have many capabilities which are yet to be explored by humans. AI is a gift to human civilization. But at the same time, AI is being used by attackers also to attack and exploit the system and access all possible kind of data, privileges and ransom. ML needs to be trained in such a way that it can be used for restricting cyber-attacks. Because for now, cyber war is the new battlefield. And AI and ML are the golden keys to achieve the victory.

DOI: 10.17148/IARJSET.2021.8557

REFERENCES

[1]. Arockia Panimalar.S, Giri Pai.U, Salman Khan.K, “ARTIFICIAL INTELLIGENCE TECHNIQUES FOR CYBER SECURITY:, Volume: 05 Issue: 03, International Research Journal of Engineering and Technology (IRJET), March 2018.

[2]. Pandey, M. (2018). Artificial Intelligence in Cyber Security. On Emerging Trends In Information Technology (NCETIT’2018) with the theme- ‘The Changing Landscape Of Cyber Security: Challenges, 66

[3]. Azzah Kabbas, Atheer Alharthi , and Asmaa Munshi, “Artificial Intelligence Applications in Cybersecurity”, IJCSNS International Journal of Computer Science and Network Security, VOL.20 No.2, Fabruary 2020.

[4]. https://www.simplilearn.com/tutorials/artificial-intelligence-tutorial/types-of-artificial-intelligence

[5]. Sagar Samtani, Murat Kantarcioglu, Hsinchun Chen, “Trailblazing the Artificial Intelligence for Cybersecurity Discipline: A Multi-Disciplinary Research Roadmap,” ACM Transactions on Management Information Systems, Vol. 11, No. 4, Article 17, December 2020.

[6]. https://www.researchgate.net/publication/330569376_The_Role_of_Artificial_Intelligence_in_Cyber_Security

[7]. https://www.omnisci.com/

[8]. Patil Amit , Mahind Rupali , A Review Paper on General Concepts of “Artificial Intelligence and Machine Learning”, National Conference on Innovative Applications and Research in Computer Science and Engineering (NCIARCSE-2017),IARJSET, Vol. 4, Special Issue 4, January 2017

[9]. Isaac Wiafe , Felix Nti Koranteng , Emmanuel Nyarko Obeng, “Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature,”IEEE Access, July 30, 2020.

BIOGRAPHY

The Author is currently working as a software engineer and a cyber-security analyst at Infosys and has technical experience of working on real time cyber security projects and AI,ML programming since past 2 years. The Author has completed Bachelor of Engineering (BE) in Computer Science and Engineering from Dr.AGTI’ Dr. Daulatrao Aher College Of Engineering, Karad, India in 2019. Author has sincere interest and work portfolio in machine learning, AI and cyber security.