AI For CyberSecurity

Galiveeti Poornima[1], Dr. Deepak S Sakkari[2], and Dr. Pallavi R[3]

[1]Asst. Prof, Dept. of CSE, Presidency University
[2]Asst. Prof, Dept. of CSE, Sri Krishna Institute of Technology
[3]Asst. Prof, Dept. of CSE, Presidency University

Abstract

In recent digital age, Cyber Security has boomed to priority tip. Security concerns viz. Data Breaches, ID theft, Captcha Hacking, and other similar situations have emerged as harmful data threat to the society. Challenge in designing appropriate rules and process and applying the same on c2itical data threat scenarios to perfectly combat cyberattacks and crimes are limitless. Recent developments in Artificial Intelligence (AI) have resulted in a dramatic escalation of the ever-increasing threat posed by cybercriminals and attacks. It has been used in practically all branches of engineering and research. AI has ushered forth a revolution in everything from robots to healthcare. Cybercriminals were unable to avoid this ball of fire, and as a result, "ordinary" cyberattacks have evolved into "intelligent" ones. In the subject of cybersecurity, AI can serve as a foundational tool because of its ability to adapt quickly to new scenarios. AI-based techniques can be used to identify malware assaults, network intrusions, phishing and spam emails, and data breaches, among other things, and to warn security incidents when they occur.

I Introduction

Even though many people have intellect, a significant number of them do not have the capabilities of ways to appreciate an issue and discover solutions for it. In terms of decreasing operational errors and finding inconsistencies, AI is ahead of human ability and expertise. Artificial intelligence is essential in assessing errors that individuals are powerless to avoid(Sadiku, Fagbohungbe, & Musa, 2020). Artificial intelligence as a cybersecurity solution can assist protect businesses from online attacks, identify different virus types, ensure practical security standards, and improve anticipation and recovery systems. Thus, we will shed light on how AI developments and applications might strengthen security through our investigation (Patil, 2016).

The security of cyberspace has had a considerable influence on a number of the key frameworks that are in use today. Traditional security (Morovat & Panda, 2020) relies on static management of security devices provided to unusual edges or hubs, such as firewalls, intrusion detection systems (IDSs), and intrusion prevention systems (IPSs), for network security according to the preset criteria (Patil, 2016).

Integrating Artificial Intelligence into existing cybersecurity frameworks has the potential to mitigate the ever-increasing and expanding threats to data security that are now confronted by global enterprises. Machine Learning and Artificial Intelligence (AI) (Farrukh & Khan, 2021) are currently more widely associated with businesses and applications than at any other time in recent memory as registering power, storage limits, and information data gathering augment. It is impossible for a single person to logically handle such a large quantity of knowledge. By using Machine Learning and AI, we can perhaps shrink that informational mountaintop over time, allowing systems to detect and recover from security threats.

Since recent events have shown that malware and cyber-weapons are getting smarter and smarter quickly, it is reasonable to think that only smart code will protect against smart cyber bats. The stakes of cyber events are raised by the use of organization-centric warfare, calling for novel ways to cyber defence. New security measures, such as the tight design of guarded perimeters, in-depth situational awareness, and highly automated response to threats in businesses, need the use of artificial intelligence (AI) methods and knowledge-based tools and technology. Why has the intelligent coding component of cyberwork expanded at such a rapid pace?

Closer proximity to the cyber house will reveal the resulting response. A realistic response to issues on the internet requires artificial intelligence. One should be able to deal with the unusual arrangement

of information in a matter of seconds to clarify and separate functions that occur in the cybersecurity environment and to make time-based decisions. Humans are incapable of keeping up with the cycle time and data utilisation required without major automation. But it's hard to create code with standard algorithms that can protect against attacks in cybersecurity because new threats keep coming up all the time (Donepudi, 2015).

II Types of Cyber Attacks

A cyber-attack occurs when an outside entity gains access to a computer or network without permission. One who commits a cyberattack is referred to as a hacker or attacker. Cyberattacks have a number of detrimental repercussions. Data breaches, the loss or alteration of information as a result of an attack, are a real possibility. Companies suffer financial losses, a decrease in customer trust, and even reputational harm. We employ cybersecurity to prevent cyberattacks. Network, computer, and their component protection from unwanted digital access is known as cybersecurity. The state of cyber security has also been weakened by the COVID-19 era. Cyberattacks have increased significantly during the COVID-19 pandemic, according to Interpol and WHO.

Currently, cyberattacks come in a wide variety of forms. It is much simpler for us to defend our networks and systems against different kinds of assaults if we have a solid understanding of those attacks. We'll look at top cyberattacks that can damage an individual or a major business.

- **Malware Attack**(Sadiku et al., 2020): Such assaults are quite common in the cyber world. Malware is an umbrella term for a variety of different types of malicious software viruses, including worms, spyware, ransomware, adware, and Trojan horses. The malicious programme masquerades as something else entirely. Unlike Spyware, which takes your personal information in the background without your awareness, Ransomware prohibits you from accessing critical sections of your network. Adware is defined as software that displays banner adverts and other forms of commercial material on the screen of a user. When a user clicks on a risky link, opens an email attachment, or uses a pen drive that has been infected, a vulnerability is exploited by malware to access the network.

  Now let's examine how to stop a malware attack:

  * Utilize some sort of antiviral software. It can safeguard your machine against infection. The antivirus software packages McAfee, Norton, and Avast are among the most well-known names in the industry.
  * Employ firewalls. The traffic that might enter your device is filtered by firewalls. The default built-in firewalls for Windows and Mac OS X are referred to as Windows Firewall and Mac Firewall, respectively.
  * Stay vigilant and refrain from clicking on shady links.
  * Maintain regular OS and browser updates.

- **Phishing Attack**(Samtani, Kantarcioglu, & Chen, 2020): Phishing is a common cyberattack. One method of social engineering is to pose as a recipient's friend or colleague in an email to persuade them to click on a link that really contains malware. The victim does not realise what is happening and proceeds to open the email, at which point they either click on the malicious link or open the infected attachment. A successful assault like this allows the bad guys to obtain your private data and login credentials. Another way they can spread malware is through phishing scams.

  By following the recommendations below, phishing attacks can be avoided:

  * Examine the emails you get carefully. Common flaws found in phishing emails include misspelt words and altered layouts compared to official businesses.
  * Use a toolbar that detects phishing attempts.
  * In order to keep your accounts secure, you should change your passwords frequently.

- **Password Attack**(Mohammed, 2020): It's a type of cyberattack in which an attacker attempts to get access to your system by deciphering your password using software and hardware designed specifically for that purpose. Assaults on a user's password can take several forms, including brute force attacks, dictionary attacks, and keylogger attacks, among others(Mallik, 2019).

  Here are a few strategies for guarding against password attacks:

    - Create secure passwords with a combination of letters, numbers, and special characters.
    - It is strongly recommended that you do not use the same password for several websites or accounts. Instead, you should use passwords that are exclusive to each account.
    - Update your passwords to reduce the risk of a password attack.
    - Keep any password suggestions hidden from view.

- **Man-in-the-middle Attack**(Farrukh & Khan, 2021; Sadiku et al., 2020): Eavesdropping is another name for a Man-in-the-Middle attack, which is abbreviated to "MITM." In this attack, an attacker intervenes in a two-party communication, i.e., the attacker hijacks the session between a client and a host. Data is taken by hackers and then altered in this manner.

  The methods outlined below will help you avoid being a victim of a MITM attack:

    - While you are using the website, you should keep in mind the importance of maintaining its security. Implement encryption on your various pieces of hardware.
    - Avoid utilising open Wi-Fi networks.

- **SQL Injection Attack**(Bhatele, Shrivastava, & Kumari, 2019): When a hacker alters a standard SQL query on a database-driven website, it results in a Structured Query Language (SQL) injection attack. It does this by putting malicious code into an open search box on a website, which then compels the server to provide private information. This provides the attacker with the ability to read, change, and delete the tables in the database. Attackers may also do so to get administrative access.

  Defend against a SQL injection attack by:

    - Utilize an intrusion detection system, as they are made to identify unwanted network access.
    - Validate the information that the user has provided. By using a validation procedure, it controls user input.

- **Denial-of-Service Attack**(Kuzlu, Fair, & Guler, 2021): An assault known as a denial-of-service, or DoS, presents a significant threat to organisations. Attackers go after systems, servers, or networks and flood them with traffic to use up their bandwidth and resources. When this occurs, the server (or servers) that are hosting the website either completely stop functioning or encounter major slowdowns because the number of requests that they are expected to handle becomes too high. Therefore, legitimate demands for assistance are ignored. This kind of attack is sometimes referred to as a DDoS attack, which stands for "distributed denial-of-service." A DDoS attack occurs when an adversary launches an assault by using a large number of computers that have been compromised.

  Now let's examine how to stop a DDoS attack:

    - Conduct an analysis of the traffic in order to identify any malicious activity.
    - Recognize the warning indications, such as a sluggish network and intermittent problems with the website. In circumstances like this, the organisation has to take immediate action.
    - Make sure your data centre and personnel are ready to handle a distributed denial of service assault by developing a plan and keeping a checklist.
    - Contract with cloud-based service providers to prevent DDoS.

- **Insider Threat**(Mallik, 2019): An insider threat is a threat that originates from within an organisation, as the term suggests. In this situation, it can be someone who works for the company and is well-versed in its operations. Threats that originate from within an organisation have the ability to do enormous amounts of damage. When employees of a small business have access to several accounts, the company is vulnerable to insider threats. This type of attacks can be motivated by anything from simple greed to deliberate maliciousness or even simple negligence. Insider threats are tricky because they are difficult to predict.

  In order to avoid an insider threat attack:

    - It is important for companies to develop a strong culture of security awareness throughout their organisations and people.

    * Companies must limit the IT resources that employees have access-to based on their job duties.
    * Employers must train their staff to recognise insider risks. This will make staff more aware of when a hacker has tampered with or is attempting to misuse the organization's data.

- **Cryptojacking**(Patil, 2016; Calderon, 2019): Cryptojacking is a phrase that has a lot to do with cryptocurrencies. When hackers get access to another person's computer to mine cryptocurrencies, this is known as cryptojacking. By infecting a website or tricking the victim into clicking on a malicious link, access is achieved. For this, they also use JavaScript-coded internet advertisements. As Crypto mining code runs in the background, victims are oblivious; a delay in execution is the only clue.

  Following the below-mentioned procedures will prevent cryptojacking:

    * It is important to keep your operating system and all of your security applications up-to-date because cryptojacking can affect even the most poorly protected computers.
    * Employees can be better prepared to identify cryptojacking threats if they are given cryptojacking awareness training.
    * Install an ad-blocker because advertising are the main source of scripts used for cryptojacking. They have additional extensions like MinerBlock, which is used to recognise and stop scripts that mine for cryptocurrency.

- **Zero-Day exploit**(Calderon, 2019): A Zero-Day Exploit occurs after a network vulnerability has been disclosed, but before a patch has been released. As a result, the vendor alerts consumers to the vulnerability; nevertheless, the info also reaches the attackers. The vendor or developer may need any amount of time to address the problem, depending on the severity of the vulnerability. Meanwhile, exposed vulnerability is the focus of the attackers. They make sure to take advantage of the vulnerability even before a patch or other fix is put in place.

  Zero-day vulnerabilities can be avoided by:

    * It is important for companies to have patch management procedures that are clearly explained. Applying management solutions that automate the processes will improve efficiency. That means deployment won't be slowed down.
    * Prepare an incident response strategy in case of a cyberattack. Maintain a strategy that focuses on zero-day assaults. By doing this, the damage can either be minimised or even averted.

- **Watering Hole Attack**(Taddeo, McCutcheon, & Floridi, 2019): Here, a certain group inside an organisation, locale, etc., is the victim. In such an assault, the attacker picks websites that the targeted group frequents regularly. Websites are found either by attentively observing the group or by making an educated assumption. These websites are then infected with malware by the attackers, which then compromises the systems of the victims. The malicious software used in this kind of assault is aimed at the user's private information. It is also possible for the hacker to have remote access to the machine that has been compromised in this scenario.

  Now, let's check over some strategies for warding off an assault at a watering hole.

    * Update your software to lessen the chance of a hacker exploiting a weakness. Make sure you routinely check for security fixes.
    * In order to recognise watering hole attacks, use your network security tools. When it comes to identifying these suspicious actions, intrusion prevention systems (IPS) are effective.
    * To prevent a watering hole assault, it is recommended to mask online actions. Use a VPN and your browser's private browsing function to accomplish this. A virtual private network, or VPN, encrypts your connection to another network so that it can travel across the public Internet. It serves as a guard for your online browsing. A VPN that works well is NordVPN.

III How AI is Used in CyberSecurity

When we talk about artificial intelligence in relation to cyber security, this is not a novel topic. Indeed, two years ago, people would discuss how artificial intelligence and machine learning in cyber security would transform the future, as data is at the heart of cyber security trends.

AI proves useful in the field of cyber security by enhancing the investigation, analysis, and comprehension of cybercrime by professionals. It advances the tools businesses use to fight cybercrime and aids businesses in protecting client data. However, artificial intelligence can also be a very comprehensive resource and might not be practically suitable in every application. Most importantly, it can also be used by hackers as a new weapon to hone their skills and strengthen their cyberattacks.

With less resources available to them, security operations analysts are using AI to stay ahead of the more sophisticated cyberattacks. AI technologies, like machine learning and natural language processing, rapidly glean insights to cut through the noise of daily alerts and significantly shorten response times by curating threat intelligence from millions of research papers, blogs, and news reports.

IT security professionals may employ AI and ML to enforce good cybersecurity practises and decrease the attack surface. At the same time, state-sponsored attackers, criminal cyber-gangs, and ideological hackers are all capable of utilising those same AI techniques to circumvent detection and overcome defences. The "AI/cybersecurity problem" is present here. Companies will need to be on the lookout for the potential drawbacks of this innovative new technology as AI develops and progressively infiltrates cybersecurity:

- Machine learning and artificial intelligence can help protect against cyber-attacks, but hackers can defeat security algorithms by targeting the data they train on and the warning flags they search for.
- Additionally, hackers can create evolving malware that alters its structure to evade detection and circumvent protections by using AI.
- Without access to vast quantities of data and events, artificial intelligence systems will provide erroneous conclusions and false positives.
- If data manipulation goes unnoticed, businesses would struggle to recover the accurate data that powers their AI systems, which could have fatal results.

IV Benefits of Using AI for CyberSecurity

The goal of artificial intelligence is to mimic human intelligence. The potential for cybersecurity is enormous. Artificial intelligence (AI) systems can be taught to produce alerts for dangers, recognise novel malware strains, and safeguard critical data for organisations if properly harnessed.

A midsized organisation receives notifications for more than 200,000 cyber events every day, according to TechRepublic. It is impossible for a normal company's team of security specialists to handle the volume of threats that are now present. As a result, some of these dangers will unavoidably go undetected and seriously harm networks.

AI is the best cybersecurity solution for companies today that want to succeed online. Security professionals require smart robots and AI to safeguard their organisations from cyber threats. The advantages of combining cybersecurity and AI are as follows:

- **A**I evolves

  AI technology improves network security over time. Machine learning and deep learning are used to figure out how a business network acts over time. It can detect trends on the network and group related nodes together. It detects deviations or security issues before responding. The patterns that AIs learn over time can be used to make systems more secure in the long run. Similar dangers are blocked early. Hackers can't beat AI because it keeps learning.

- **A**I identifies undiscovered threats

  A human can't identify all a company's dangers. Hackers launch millions of attacks each year. Unknown dangers can destroy networks. Worse is their impact before they're detected, identified, and prevented. Because attackers are constantly trying new methods, ranging from complex social engineering to malware attacks, it is essential to employ contemporary solutions in order to stop them. AI is one of the greatest security technologies for mapping and stopping unforeseen threats.

- **A**I is data-savvy

  The network of a corporation sees a significant amount of daily activity. Huge amounts of foot traffic are typical for companies of a typical midsize. What this means is that there is constant

communication between the company and its clientele. This information needs to be protected from dangerous software and individuals. However, cybersecurity specialists cannot inspect all traffic for potential attacks. Artificial intelligence

- (AI) is the finest solution that will assist you discover any threats that are hiding in behaviour that appears to be regular. Because it is automated, it is able to skim through vast amounts of data and traffic without difficulty. Robotic artificial intelligence (AI) technology, such as a home proxy, can facilitate data transit. Additionally, it is able to detect and recognise any potential dangers that may be masked by the chaotic flow of traffic.

- **B**etter Vulnerability Management

  Management of vulnerabilities is one of the most important aspects of safeguarding a company's network. As was just discussed, the typical business faces a multitude of dangers on a regular basis. In order to ensure it is secure, it must detect, identify, and prevent them. Analyzing and reviewing existing security mechanisms using AI research can aid in vulnerability management. AI makes it possible to evaluate more quickly than cybersecurity personnel, which significantly improves your ability to find solutions to problems. It does this by locating weak places in computer systems and corporate networks and by assisting organisations in concentrating their attention on the most vital security responsibilities. Because of this, it is now feasible to monitor vulnerabilities and ensure the security of business systems in a timely manner.

- **B**etter Overall Security

  Business networks are occasionally exposed to new risks. Every day, hackers come up with new strategies. This makes it challenging for businesses to set priorities for security tasks. You might have to deal with phishing, ransomware, and denial-of-service att acks all at once. These assaults have comparable potential, but you must first determine how to defend yourself against each one. Errors and lapses in on the part of humans are far more likely to compromise security. Utilizing AI to detect all forms of attacks, assist in their prioritisation, and aid in their prevention is the answer in this situation.

- **R**educe duplication

  As was already stated, assailants frequently switch up their strategies. The fundamental security best practises, however, never change. If you pay someone to complete these activities, they can become disinterested throughout. Alternately, they can be worn out and complacent and neglect a crucial security responsibility, exposing your network. AI mimics the greatest human attributes and leaves out the flaws handle duplicative cybersecurity tasks. It assists in regularly monitoring for fundamental security threats and preventing them. Additionally, it performs a thorough analysis of your network to look for security flaws that can be detrimental to it.

- **S**ecuring Auth

  Most websites have a login feature to access services or buy things. Some feature contact forms with sensitive info. A corporation needs an extra security layer to manage a site with personal data and sensitive information. The extra security layer will protect your network's visitors. AI safeguards account logins. AI identifies using facial recognition, CAPTCHA, and fingerprint scanners. These attributes can assist detect a fake login attempt. Hackers enter company networks through credential stuffing and brute force. Once an attacker enters a user account, your network is at risk.

- **R**apid detection and response

  Threat detection begins network security. Untrusted data should be readily discovered. It prevents network damage. Integrating artificial intelligence (AI) into cybersecurity is the most effective method for spotting potential dangers and launching rapid responses against them. Your entire system is analysed by the AI, and it looks for any potential dangers it may have detected. AI identifies dangers early and simplifies security processes.

V Use Cases of AI CyberSecurity

Cybercriminals use AI to plan smarter, more successful assaults. Cybersecurity companies should use AI to safeguard themselves. "Organizations can't bring knives to gunfights," argues Mimecast's Dr. Herbert Roitblat.

AI in cybersecurity can also help overworked and understaffed cyber services decipher threats so they can focus on higher-order duties. Cyber leaders are anticipated to increase spending on systems that incorporate artificial intelligence. According to Meticulous Research, the global market for AI cybersecurity technologies is expected to increase at a compound annual rate of 23.6% through 2027, when it will reach $46.3 billion.

- **The detection of spam and social engineering**

  As a branch of machine learning, deep learning is a statistical method that gives computers the ability to tackle problems that were previously impossible for them to handle. It is more effective than "shallower," supervised machine learning, which instructs the computer by using labelled data to learn by example. Instead, deep learning uses massive amounts of data to "train" a deep neural network, which then gradually teaches itself new skills such as picture recognition or task completion. Deep learning models can obtain excellent accuracy rates even for ill-defined assault actions. They are used to recognise photos that are unfit for work and other images (such logos), as well as to more effectively identify spam email and phishing efforts. Deep learning has been employed by Google to filter emails containing difficult-to-detect picture (Vincent, 2019).

- **Detecting Anomalies**

  One of the most beneficial applications of machine learning for information security is the identification of complex patterns. Cyber attackers frequently conceal themselves within networks and avoid discovery by encrypting their connections, using credentials that have been stolen, and deleting or altering logs. A machine learning system, however, can still spot them in the act because it is made to identify strange behaviour. Since machine learning is so good at finding patterns in data, it can detect anomalies that manual methods may have missed. By continuously monitoring network traffic for deviations, for instance, (Teoh et al., 2018) a machine learning model can identify dangerous patterns in email sending frequency that may indicate the usage of email for an outbound assault. Additionally, models can be set up to monitor insider risks. (Tuor, Kaplan, Hutchinson, Nichols, & Robinson, 2017) In addition, machine learning is capable of adjusting to changes by absorbing new data and to changing circumstances.

- **Keeping DNS Data From Being Exfiltrated**

  The goal of malicious actors is to get past current cyber defences like firewalls and intrusion detection and prevention systems. Domain name system (DNS), the internet's database of addresses, might be a "weak link in cybersecurity procedures," according to Black Hat. (Marrison, 2015) By spoofing DNS traffic, hackers can infect users' devices, seize control of their systems, and steal personal information such as email addresses and credit card numbers that would otherwise be blocked by a firewall. (van Leijenhorst, Chin, & Lowe, 2008) Black Hat asserts that using models that are continuously trained on the trillions of DNS queries that are created and gathered each day globally, machine learning can identify and prevent so-called "DNS tunnelling" for data exfiltration.

- **Advanced Malware Detection**

  Malware detection has typically entailed keeping an eye on and scanning through network data for signature matches, or resemblances to recognised symptoms of compromise. (Farrukh & Khan, 2021) However, deep learning offers the chance to examine vast amounts of data to draw conclusions about malware before it is ever opened. Deep learning models can keep up with malware's rapid evolution. In fact, according to SearchSecurity, "the availability of tens of millions of labelled samples from both malware and innocuous applications have proven this one of the most successful implementations of deep learning and AI in cybersecurity." (Groopman, n.d.).

- **Prevention of Alert Fatigue**

  Artificial intelligence (AI) in cybersecurity can prevent the security operations centre (SOC) personnel from becoming overburdened by constant incident alerts. Machine learning can be used to prioritise low-risk alerts, automate routine processes, and improve the threat intelligence thresholds that require human involvement. (Johnson, 2019)Experts in the field of security analysis and monitoring will never be replaced by machines, but the latter may allow them to devote more time to strategic planning and analysis. Recently, an MIT startup created a closed loop methodology, in which machine learning models alert users to potential assaults, human analysts investigate them,

and the model then incorporates the results. Security analysts can work more efficiently, and the algorithm can gradually improve its performance. (Winn, 2020)

- **Tracking down Zero-Day Exploits**

  One of the greatest issues facing modern cybersecurity is preventing attacks that take use of vulnerabilities that have not yet been publicly disclosed. In a zero-day attack, attackers use software flaws that vendors are unaware of (or have not yet addressed) to inject malware. Since zero-day exploits are so novel, they can't be detected by signature-based endpoint security products like antivirus software or patch management solutions. But AI might be useful. Deep learning architectures can be used to discover hidden or latent patterns and become more context-aware over time, both of which are helpful in finding zero-day vulnerabilities or activities. Deep learning architectures can also be used to reveal hidden or latent patterns. The processing of natural languages can examine source code to identify potentially harmful files. It's possible that "generative adversarial networks," which can be trained to simulate any data distribution, will be useful in identifying sophisticated flaws. From a different perspective, a team from Arizona State University employed machine learning to track dark web traffic and find information about zero-day exploits. Since then, they've established a firm that use cutting-edge machine learning algorithms to forecast which software flaws criminal actors would most likely target next using information gathered from thousands of their posts and debates (Zhou & Pezaros, 2019).

VI Conclusion

Predictive analysis to identify anomalous/ suspicious behavioural patterns of activities is one of the most used application of Artificial Intelligence and thus holds a perfect fit in the field of Cyber Security. Cyber criminals are always on the outlook of exploiting systems through new trends. AI which endeavours to simulate human intelligence can identify these new treats before they attempt to cause a collateral damage. AI can be encapsulated with eight major benefits viz. dynamic learning, identifying unknown treats, able to handle big data, better vulnerability management, better overall security, duplicative process reduction, accelerated detection and response times and security authentication. These features of AI have an immense potential in the field of cybersecurity.

References

Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019, 01). The role of artificial intelligence in cyber security. In (p. 170-192). doi: 10.4018/978-1-5225-8241-0.ch009

Calderon, R. (2019). The benefits of artificial intelligence in cybersecurity.

Donepudi, P. K. (2015). Crossing point of artificial intelligence in cybersecurity. *American journal of trade and policy*, *2*(3), 121–128.

Farrukh, Y. A., & Khan, I. (2021). An autonomous self-incremental learning approach for detection of cyber attacks on unmanned aerial vehicles (uavs). *arXiv preprint arXiv:2112.11219*.

Groopman, J. (n.d.). *Understand the top 4 use cases for ai in cybersecurity.*

Johnson, J. (2019). Artificial intelligence & future warfare: implications for international security. *Defense & Security Analysis*, *35*(2), 147–169.

Kuzlu, M., Fair, C., & Guler, O. (2021). Role of artificial intelligence in the internet of things (iot) cybersecurity. *Discover Internet of things*, *1*(1), 1–14.

Mallik, A. (2019). Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, *2*(2), 109–134.

Marrison, C. (2015). Understanding the threats to dns and how to secure it. *Network Security*, *2015*(10), 8–10.

Mohammed, I. A. (2020). Artificial intelligence for cybersecurity: A systematic mapping of literature. *INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]*, *7*(9).

Morovat, K., & Panda, B. (2020). A survey of artificial intelligence in cybersecurity. In *2020 international conference on computational science and computational intelligence (csci)* (pp. 109–115).

Patil, P. (2016). Artificial intelligence in cybersecurity. *International journal of research in computer applications and robotics*, *4*(5), 1–5.

Sadiku, M. N., Fagbohungbe, O. I., & Musa, S. M. (2020). Artificial intelligence in cyber security. *International Journal of Engineering Research and Advanced Technology*, *6*(05), 01–07.

Samtani, S., Kantarcioglu, M., & Chen, H. (2020). *Trailblazing the artificial intelligence for cybersecurity discipline: a multi-disciplinary research roadmap* (Vol. 11) (No. 4). ACM New York, NY, USA.

Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence*, *1*(12), 557–560.

Teoh, T., Chiew, G., Franco, E. J., Ng, P., Benjamin, M., & Goh, Y. (2018). Anomaly detection in cyber security attacks on networks using mlp deep learning. In *2018 international conference on smart computing and electronic enterprise (icscee)* (pp. 1–5).

Tuor, A., Kaplan, S., Hutchinson, B., Nichols, N., & Robinson, S. (2017). Deep learning for unsupervised insider threat detection in structured cybersecurity data streams. *arXiv preprint arXiv:1710.00811*.

van Leijenhorst, T., Chin, K.-W., & Lowe, D. (2008). On the viability and performance of dns tunneling.

Vincent, J. (2019). Gmail is now blocking 100 million extra spam messages every day with ai. *The Verge*.

Winn, Z. (2020). A human-machine collaboration to defend against cyberattacks. *Technology. org*.

Zhou, Q., & Pezaros, D. (2019). Evaluation of machine learning classifiers for zero-day intrusion detection–an analysis on cic-aws-2018 dataset. *arXiv preprint arXiv:1905.03685*.