**Artificial Intelligence Impact Cyber Security**

What are the most important apps on your smartphone? Maybe it is your bank app? Or even your Gmail account? Whatever important app it is, chances are it is password protected or secured in multiple ways. This cybersecurity becomes even more important in a professional setting where your company account has multiple barriers such as antivirus, password protection, etc. These are all elements of cybersecurity that are extremely necessary to secure both your personal and professional accounts from malicious users and hackers.

But conventional cybersecurity methods are not enough these days. Hackers can access accounts remotely and cause data breaches, identity thefts, loss of money, etc. In this data age, data is the most unsafe and easily targeted commodity. In such a situation, **Artificial Intelligence** can provide immense help to the cybersecurity industry, especially since many cybercriminals are already using this technology. As they say, it is only possible to fight fire with fire! But how can artificial intelligence be so important in cybersecurity? Let’s understand this in detail and then see the applications of artificial intelligence in cybersecurity.

**Why is Artificial Intelligence so important in Cyber Security?**

Artificial Intelligence is a double-edged sword in cybersecurity. There is a lot of concern that hackers can use AI to automate cyber-attacks while simultaneously reducing the numbers of humans needed. After all, if there are complex AI algorithms then hackers need fewer people to coordinate and implement their cyber-attacks which have more chances of being successful. Another advantage that AI provides hackers is that it is much easier to find out system vulnerabilities and attack networks such that the attacks are never even recognized.

There are many facets of cybersecurity in which AI can have multiple applications such as intruder detection, prevention of phishing attacks, user behavior analysis, etc. Let’s see these in detail now:

**1. Intruder Detection**

Artificial Intelligence methods can be a big help in the field of intruder detection in cybersecurity. They can help in detecting and defending against any intruders in the system using past insights into intruder activity patterns. For example, intruders in the system may be engaging in unnatural behaviors such as sending and receiving large amounts of data or suddenly changing the communication patterns. These signs of intruders in the system are very difficult to catch for cybersecurity professionals, especially in large companies where there is a lot of network traffic. Here, the AI-powered intruder detection systems can be used to monitor the network for any unwanted intruders.

**2. User Behavior Analysis**

Sudden changes in the behaviors of existing users can be a sign of a cyber-attack in the network. This could happen if a malicious user stole the login credentials of a legitimate user and then illegally logged into the network using those credentials. But these behavioral changes are extremely hard to identify, especially in a large network. In such a situation, artificial intelligence can be used to detect and block the compromised user accounts which depict suspicious behavioral changes. AI can do this by creating a user behavioral profile of all the users which includes their login and logout patterns, data transfer patterns, etc. Then user behavior analysis on these profiles can help in identifying whenever a user behaves out of their normal behavioral profile which can be used to alert the cybersecurity team that something is out of the ordinary.

**3. Prevention of Phishing Attacks**

Artificial Intelligence can also be extremely helpful in preventing phishing attacks on users in a particular network. These phishing attacks are extremely common in many companies where the employees are sent fraud Emails with the intention of obtaining their company sensitive information such as company passwords, their banking and credit card details, etc. Artificial Intelligence methods such as Natural Language Processing can be used to monitor the employee Emails in their company account and see if there is anything suspicious such as some patterns and phrases that may indicate that the Email is a phishing attempt. This is an extremely important application of AI as phishing attempts are extremely common, so much so that every 1 in 99 Emails might be a phishing attempt.

**4. Antivirus Software**

Traditional antivirus software may not be able to keep up with all the changes to viruses, especially AI-enhanced viruses that are cropping up these days. This is because antivirus software protects the system by scanning all the files on the network to identify if they might actually match with a known virus or malware signature. But this is very difficult to do if the known viruses keep changing and evolving continuously. In that situation, it is best to use Antivirus software that is integrated with artificial intelligence. This type of antivirus detects viruses in the system not by checking if they match with a known virus or malware signature but by identifying their abnormal behavior that is outside the current window of normality for the network. AI-based antivirus systems can do this by leveraging mathematical AI algorithms and data science as well.

**5. Password Protection**

Password protection is an integral part of cybersecurity. After all, many times passwords are the only things standing between a hacker and complete access to the account. However, sometimes passwords are not adequate protection for companies. There may be employees that have very simple passwords on their accounts or even have the same password for different type accounts. So hacking those accounts is a child’s play for hackers. In such situations, Artificial Intelligence can be used to provide much better password protection by using features such as facial recognition for opening the accounts. The facial recognition technology can use infra-red sensors and neural networks to map out the distinct patterns on each individual face so that only they are able to open their account and no one else. This advanced AI facial recognition technology can also account for changes such as different hairstyles, wearing a hat, etc. so that no one can fool the system and enter the account illegally.

## **Application of AI And Machine Learning in Cybersecurity**

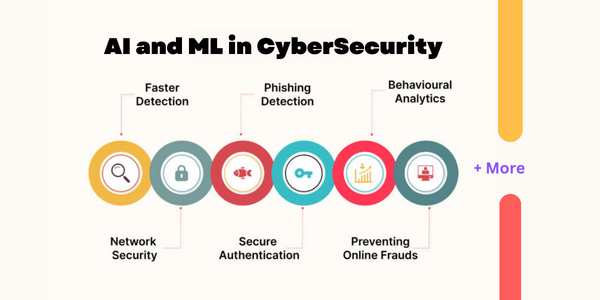
Here is a few potential application of AI and Machine Learning in Cybersecurity,

**1. Using Machine Learning for Malware Detection and Classification**

Another area where AI and ML are used in cybersecurity is [detecting and classifying malware](https://www.analyticsvidhya.com/blog/2022/01/microsoft-malware-detection/). Machine learning algorithms can be trained to recognize the characteristics of different types of malware, such as viruses, worms, and trojans. This enables the system to detect and classify new malware in real-time, even if it has not been previously seen. You can [also read](https://www.analyticsvidhya.com/blog/2020/09/machine-learning-in-cyber-security-malicious-software-installation/)this article for more information.

**2. Adversarial Machine Learning and its Implications for Cybersecurity**

Adversarial machine learning is another area of AI and ML that has implications for cybersecurity. This approach involves training machine learning models to recognize and defend against adversarial examples, which are inputs specifically crafted to fool the model. In cybersecurity, adversarial machine learning can be used to detect and defend against adversarial attacks, such as those that attempt to evade intrusion detection systems or fool a system into misclassifying malware as benign.



**3. AI-based Network Traffic Analysis and Anomaly Detection**

AI and ML are also used in network traffic analysis and [anomaly detection](https://www.analyticsvidhya.com/blog/2023/01/impact-of-categorical-encodings-on-anomaly-detection-methods/). These systems use machine learning algorithms to analyze network traffic and detect anomalies, which may indicate a potential intrusion. For example, a system can use ML to detect a sudden increase in traffic from a specific IP address or to identify network activity patterns indicative of a particular type of attack.

**4. AI-assisted Penetration Testing and Vulnerability Management**

Penetration testing and vulnerability management are also areas where AI and ML are used. Penetration testing is the process of attempting to gain unauthorized access to a system or network. At the same time, vulnerability management is the process of identifying, evaluating, and mitigating vulnerabilities in a system or network. [Machine learning algorithms](https://www.analyticsvidhya.com/blog/2022/07/machine-learning-aided-differentiation-of-real-and-fake-news/) can be used to automate both of these processes, making them more efficient and effective.

**5. Real-time Threat Intelligence with Machine Learning**

In cybersecurity, real-time threat intelligence is another area where AI and ML are used. These systems use machine learning algorithms to analyze data from various sources and provide real-time threat intelligence. This enables organizations to identify and respond to emerging threats quickly.

**6. AI-powered Security Automation and Orchestration**

AI-powered security automation and orchestration is another area where AI and ML are used. These systems use machine learning algorithms to automate repetitive security tasks, such as patch management and incident response. This enables organizations to free up human resources and focus on more important tasks.

**7. AI-based User and Entity Behavior Analytics**

AI-based user and entity behavior analytics (UEBA) is another area in which AI and ML are used in cybersecurity. These systems use machine learning algorithms to analyze the behavior of users and entities on a network. This enables organizations to detect anomalies and identify potential threats, such as insider threats and advanced persistent threats (APTs).

**8. AI-Powered Cyber Threat Hunting**

AI-powered [cyber threat hunting](https://www.analyticsvidhya.com/blog/2016/08/industry-insight-fighting-cyber-fraud-with-analytics/) is an emerging application of AI and ML in cybersecurity that aims to detect and respond to advanced threats that have evaded traditional security systems. The goal of threat hunting is to identify and stop malicious actors before they can cause damage to an organization.

One of the main advantages of AI-powered threat hunting is its ability to analyze large volumes of data and identify patterns that may indicate a threat. Machine learning algorithms can be trained to recognize the characteristics of different types of threats, such as malware, phishing, or Advanced Persistent Threats (APTs). This enables the system to detect and classify new threats in real-time, even if they have not been previously seen.

**9. AI And ML in Intrusion Detection and Prevention Systems**

One of the most significant ways that AI and ML are used in cybersecurity is through intrusion detection and prevention systems (IDPS). These systems use machine learning algorithms to analyze network traffic and detect anomalies, which may indicate a potential intrusion. For example, an IDPS can use ML to detect a sudden increase in traffic from a specific IP address or to identify network activity patterns indicative of a particular type of attack.

## **Future Potential of AI And Machine Learning in Cybersecurity**

The future potential of AI and ML in cybersecurity is vast and exciting. Here are a few examples of how these technologies could be used in the future to enhance the security of organizations and individuals:

1. **Autonomous Security Systems:**AI and ML could be used to create autonomous security systems that can operate independently and make decisions without human intervention. This would enable organizations to respond to threats in real-time, even if human operators are unavailable.
2. **Predictive Threat Intelligence:**AI and ML could be used to analyze data from various sources and provide predictive threat intelligence. This would enable organizations to anticipate and prepare for emerging threats before they happen.
3. **Advanced Threat Hunting:** AI and ML could be used to create advanced threat-hunting systems that can detect and respond to unknown threats. This would enable organizations to stay ahead of attackers who are constantly evolving their tactics.
4. **AI-Driven Incident Response And Forensics:**AI and ML could be used to automatically analyze data from various sources, such as network traffic, endpoint data, and logs, to identify and respond to threats in real time. This would enable organizations to contain and investigate incidents quickly.
5. **Automated Compliance And Governance:** AI and ML could be used to automate the compliance and governance process by automatically monitoring and reporting on security controls and identifying potential violations.
6. **AI-Powered Security Automation And Orchestration:** AI and ML could be used to automate repetitive security tasks, such as patch management and incident response, which would free up human resources and focus on more important tasks.
7. **The Intersection of AI And Blockchain:**Combining AI and blockchain technology could provide a more secure and decentralized approach to cybersecurity, especially in the areas of identity and access management, secure data sharing, and secure payment systems.
8. **AI-Driven Security Operations Centers (SOC):**AI and ML could be used to improve the efficiency and effectiveness of security operations centers (SOCs) by automating repetitive tasks, analyzing data from various sources, and providing real-time threat intelligence.

## **Disadvantages of Using AI And Machine Learning in Cybersecurity**

1. **High Cost:** Implementing and maintaining AI and Machine Learning systems can be expensive. Organizations must invest in the necessary hardware, software, and expertise to deploy and manage the system.
2. **Complexity**: AI and Machine Learning systems require specialized knowledge and skills to set up, configure, and operate.
3. **Dependence On Data Quality:**The effectiveness of AI and Machine Learning in cybersecurity depends on the quality of the data used to train the machine learning algorithms.
4. **Limited Scope**: AI and Machine Learning systems focus on identifying known threats, but they may not be able to detect new, unknown threats.
5. **Lack Of Transparency:**AI and Machine Learning systems use complex algorithms that can be difficult to understand and interpret.
6. **False Positive And False Negative Alerts:** Due to the complexity of the machine learning algorithms, AI and Machine Learning systems may generate many false positive and false negative alerts.
7. **Lack Of Human Oversight:** AI and Machine Learning systems can be autonomous, meaning they don’t require human intervention.
8. **Vulnerability To Adversarial Attacks:** AI and Machine Learning systems can be vulnerable to adversarial attacks, where malicious actors try to manipulate the input data to evade detection or mislead the system.
9. **Lack Of Explainability:** AI and Machine Learning systems may be unable to explain how they arrived at a decision, making it difficult to understand and trust the results.