Use of Artificial Intelligence in cyber Security

MCA II – Sem III | AI for CS – Module

Module 1: Fundamentals of AI and CS

1.2 Machine Learning Algorithms and usage

1.3 Impact of AI on Cybersecurity

1.4 AI Applications in Cybersecurity: Real-Life Examples

- 1.4.1 Security screening
- 1.4.2 Security & crime prevention
- 1.4.3 Analyze mobile endpoints
- 1.4.4 AI-powered threat detection
- 1.4.5 Detection of sophisticated cyber-attacks
- 1.4.6 Reducing Threat Response Time

1.5 Drawbacks and Limitations of Using AI for Cybersecurity

Use of Artificial Intelligence in cyber Security

Artificial Intelligence (AI) is a revolutionizing technology that has transformed the way machines and gadgets interact with humans and each other.

The term is frequently applied to the project of developing systems endowed with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalize, or learn from past experience.

Use of Artificial Intelligence in cyber Security

Research in AI has focused chiefly on the following components of intelligence: learning, reasoning, problem-solving, perception, and using language.

An AI-powered machine can recognize or sense the changes in its environment and take appropriate action automatically in order to perform its intended task.

AI leads to minimal or no human intervention as the machines are able to perform several activities on their own. The technology has impacted almost all sectors including cyber security.

The amount of online data is growing exponentially and becoming susceptible to malicious activities.

In such a scenario, it has become difficult to safeguard large chunks of data from potential threats.

Artificial Intelligence can come into play in such cases. The technology plays a crucial role in providing protection to online data.

Following are the **use of artificial intelligence in cyber security**:

Data Handling

It is cumbersome to manage an enormous amount of data produced by systems on a daily basis.

This task can be easily executed by exploiting artificial intelligence software.

Artificial intelligence can handle and process tons of data within minutes, which would otherwise takes months.

Fast Action

AI-powered systems can quickly detect the problems and take appropriate action. On the other hand, human controlled cyber security systems would take much longer time even for detecting the problem itself.

Protection

In most of the cases, cybercriminals are found to be hiding in the system for a long time. They generally wait for the right moment to attack. With the help of artificial intelligence, we can spot these hidden threats and take appropriate actions.

Time Saving and Enhance Efficiency

By exploiting artificial intelligence in cyber security, we can save a lot of time. We don't have to manage enormous amount of data, we don't have to constantly look out for cybercriminals or threats needles. This gives us more time to plan new strategies and bring out new ideas to the table in order to improve our overall security system.

Saving Resources

With the use of artificial intelligence in cyber security, we can cut out the expenses that would have been spent on the security and management of the online data. If the task of managing and protecting data is handled manually, it would require a number of people. However, with artificial intelligence, a single system can look after tons of data.

These were some of the uses of artificial intelligence in cyber security. Although artificial intelligence has so many advantages over human intelligence, it is dependent on humans. It cannot make decisions on its own. There is equal need of a human brain as it is of artificial intelligence. All software that runs on AI is designed by computer engineers. So, proficient engineers are required

Few realistic examples of AI cyber security being used to provide and improve cyber security:

- 1. Gmail uses Machine learning to filter and remove 100 million spam emails every day.
- 2. Google uses AI on the platform used to store videos, AI sends security alarms when there is any unauthorized access.
- 3. Balbix platforms use AI to protect IT infrastructure from data and security breaches.

IMPROVING CYBER SECURITY WITH ARTIFICIAL INTELLIGENCE

- **Threat Detector**: Traditional security methods can detect up to 90% of threats. A combination of both traditional and AI techniques can detect almost 100% of threats. Organizations can speed up the threat detecting process using behavioural analysis.

- **Proactive Nature of AI**: Traditional security methods can correct only the known data breaches and vulnerabilities. On the other hand, AI can recognize the user patterns and identify the vulnerabilities before they are officially reported. The proactive nature of AI helps organizations from financial losses due to data vulnerabilities.

- Traditional security methods:
- **Locks and Keys, Access Control Systems**: key cards, **Physical Access Control:** biometrics, or PINs to manage and log access to physical areas.
- **Surveillance and Monitoring**: Security Cameras, Security Guard: Trained personnel physically monitor and patrol areas to ensure safety and security.
- **Alarms and Intrusion Detection**: Intrusion Alarms, Motion Sensors.
- **Access Logs and Records**: Visitor Logs, Access Records
- **Training and Awareness**: Employee Training, **Security Awareness**
- **Security Policies and Procedures**
- **Emergency Response Plans**
- **Access Control Lists (ACLs) in Networking**

IMPROVING CYBER SECURITY WITH ARTIFICIAL INTELLIGENCE

- **Data centres**: AI can monitor various data centres. Continuous tracking capacity of AI provides details about what would increase the effectiveness and security of hardware and infrastructure. AI has the capacity to provide alarms before there is any major hardware fault so that it can be repaired in advance of any severe damage.

- **Network Security**: Network security is any activity designed to protect the integrity of computers and networks. AI enables the Security professional to learn and remove unwanted data, detect unauthorized activity, and provide network security. AI can detect network attacks that are not possible.

AI APPLICATIONS IN CYBERSECURITY WITH REAL-LIFE EXAMPLES

- Artificial intelligence (AI) and machine learning (ML) techniques are being increasingly deployed in cyber-security settings.

- Examples of critical applications include network anomaly detection, Advanced Threat Detection, Phishing Detection, Malware Detection, Faster Incident Response, Continuous Monitoring, Behavioural Analysis, Log Analysis, Predictive Analytics, biometric authentication, spam detection, and data analytics-based financial fraud detection.

- At the same time, advanced ML algorithms also give attackers an advantage, setting up a complex interplay between attackers and defenders.

AI APPLICATIONS IN CYBERSECURITY WITH REAL-LIFE EXAMPLES

- ML systems are susceptible to new attacks.
- For instance, Adaptability of Attackers, Complexity of ML Models, Data Poisoning, Transferability, and Model Updates.
- Deep neural networks and ML “backdooring” attacks that compromise the training process. (adversarial attack where an attacker manipulates the training process or model in such a way that it includes a hidden or "backdoor" vulnerability.)
- For instance, **Poisoned Data Injection, Backdoor Trigger, Training Process, Testing Phase**
- For these reasons, there is growing interest in techniques to develop and deploy verifiably safe and secure ML systems, adopting and adapting techniques from the software security domain.

MACHINE LEARNING AND CYBER SECURITY

- Machine learning (ML) is AI's brain
- A type of algorithm that enables computers to analyze data, learn from past experiences, and make decisions, all in a way that resembles human behavior.
- Machine learning algorithms in cybersecurity can automatically detect and analyze security incidents.
- Some can even automatically respond to threats.
- Eg: Many modern security tools, like threat intelligence.

MACHINE LEARNING ALGORITHMS

- There are many machine learning algorithms, but most of them perform one of the following tasks:
- **Regression—**
- The future values are predicted with the help of regression algorithms in Machine Learning. **Problem:** Predicting House Prices
- The input data/historical data is used to predict a wide range of future values using regression.
- Label in ML is defined as the target variable (to be predicted) and regression helps in defining the relationship between label and data points.
- Regression is a type of supervised learning in ML that helps in mapping a predictive relationship between labels and data points.
- Detects correlations between different datasets and understands how they are related to each other. You can use regression to predict system calls of operating systems, and then identify anomalies by comparing the prediction to an actual call.
- Types of regression algorithms in ML are linear, polynomial, logistic, stepwise, etc

MACHINE LEARNING ALGORITHMS

- **Clustering—**

- Clustering is an unsupervised machine learning task.
- Using a clustering algorithm we give the algorithm a lot of input data with no labels and let it find any groupings in the data it can.
- Those groupings are called clusters. A cluster is a group of data points that are similar to each other based on their relation to surrounding data points.
- Identifies similarities between datasets and groups them based on their common features. Clustering works directly on new data without considering previous examples.
- Some real world applications of clustering include fraud detection in insurance, categorizing books in a library, and customer segmentation in marketing, earthquake analysis or city planning.
- These algorithms are widely used in various applications, such as spam email detection, sentiment analysis, disease diagnosis, image recognition, and more.

MACHINE LEARNING ALGORITHMS

- **Classification—**
- The Classification algorithm is a Supervised Learning technique that is used to identify the category of new observations on the basis of training data.
- Classification algorithms learn from previous observations and try to apply what they learn to new, unseen data.
- classifies new observations into a number of classes or groups. Such as, Yes or No, 0 or 1, Spam or Not Spam, cat or dog, etc. Classes can be called as targets/labels or categories.
- Classification involves taking artifacts and classifying them under one of several labels. For example, classify a binary file under categories like legitimate software, adware, ransomware, or spyware.
- These algorithms are widely used in various applications, such as spam email detection, sentiment analysis, disease diagnosis, image recognition, and more.

- Common Classification Algorithms: There are several classification algorithms used in machine learning, including but not limited to:

- Logistic Regression
- Decision Trees
- Random Forest
- Support Vector Machines (SVM)
- k-Nearest Neighbors (k-NN)
- Naive Bayes
- Neural Networks

IMPACT OF AI ON CYBERSECURITY

- While artificial intelligence can improve security, the same technology can give cybercriminals access to systems with no human intervention.

Vulnerability management

- AI and machine learning techniques can improve the vulnerability management capabilities of vulnerability databases.

For Instance: Tools like user and event behavior analytics (UEBA), when powered by AI, can analyze user behavior on servers and endpoints, and then detect anomalies that might indicate an unknown attack. This can help protect organizations even before vulnerabilities are officially reported and patched.

IMPACT OF AI ON CYBERSECURITY

- **Threat hunting**
- Conventional security tools use signatures or attack indicators to identify threats.
- This technique can easily identify previously discovered threats. However, signature-based tools cannot detect threats that have not been discovered yet. In fact, they can identify only about 90 %of threats.
- AI can increase the detection rate of traditional techniques up to 95 percent. The problem is that you can get multiple false positives. The ideal option would be a combination of AI and traditional methods. This merger between the conventional and innovative can increase detection rates by up to 100 percent, thus minimizing false positives.
- AI can also improve threat hunting by integrating behaviour analysis. For instance, you can develop profiles of every application inside your organization's network by analysing data from endpoints.

IMPACT OF AI ON CYBERSECURITY

- **Network security**
- Conventional network security techniques focus on two main aspects: creating security policies and understanding the network environment.
- **Policies**—security policies can help you distinguish between legitimate and malicious network connections. Policies can also enforce a zero-trust model. However, creating and maintaining policies for a large number of networks can be challenging.
- **Environment**—most organizations don't have precise naming conventions for applications and workloads. As a result, security teams have to spend a lot of time determining what set of workloads belong to a given application.
- AI can enhance network security by learning the patterns of network traffic and recommending both security policies and functional workload grouping.

IMPACT OF AI ON CYBERSECURITY

- **Data centres**

- AI can monitor and optimize critical data centre processes like power consumption, backup power, internal temperatures, bandwidth usage, and cooling filters. AI provides insights into what values can improve the security and effectiveness of data centre infrastructure.

- You can use AI to reduce maintenance costs. AI can prompt alerts that let you know when you have to attend to hardware failures. AI-based alerts enable you to fix your equipment before further damage occurs. Google reported a 15 percent reduction in power consumption, and a 40 percent reduction in cooling costs in their data centers, after implementing AI technology back in 2016.

AI APPLICATIONS IN CYBERSECURITY: REAL LIFE EXAMPLES

- Machine learning can quickly scan large amounts of data and analyze it using statistics.
- **Security screening**

- *An investigation for the purpose of seeing if someone can be trusted All government employees are subject to a security check.*
- Security screening done by immigration officers and customs can detect people that are lying about their intentions. However, the screening process is prone to mistakes. In addition, human-based screening can lead to errors because people get tired and can be distracted easily.
- Example: The United States Department of Homeland Security has developed a system called AVATAR that screens body gestures and facial expressions of people. AVATAR leverages AI and Big Data to pick up small variations of facial expressions and body gestures that may raise suspicion.
- The system has a screen with a virtual face that asks questions. It monitors changes in their answers as well as differences in their voice tone. The collected data is compared against elements that indicate that someone might be lying. Passengers are flagged for further inspection if they are considered suspicious.

AI APPLICATIONS IN CYBERSECURITY: REAL LIFE EXAMPLES

Security & crime prevention

The Computer Statistics (CompStat) AI system has been in use by the police department of New York since 1995. CompStat is an early form of AI that includes organizational management, and philosophy, but depends on different software tools. The system was the first tool used for “predictive policing” and many police stations across the U.S have been using CompStat to investigate crimes since then.

AI-based crime analysis tools like the California-based Armor way are using AI and game theory to predict terrorist threats. The Coast Guard also uses Armor way for port security in Los Angeles, Boston and New York.

AI APPLICATIONS IN CYBERSECURITY: REAL LIFE EXAMPLES

- **Analyse mobile endpoints**
- Google is using AI to analyze mobile endpoint threats. Organizations can use this analysis to protect the growing number of personal mobile devices.
- Zimperium and MobileIron announced a collaboration to help organizations adopt mobile anti-malware solutions incorporating artificial intelligence. The integration of Zimperium's AI-based threat detection with MobileIron's compliance and security engine can address challenges like network, device, and application threats.
- Other vendors that offer mobile security solutions include Skycure, Lookout, and Wandera. Each vendor uses its own AI algorithm to detect potential threats.

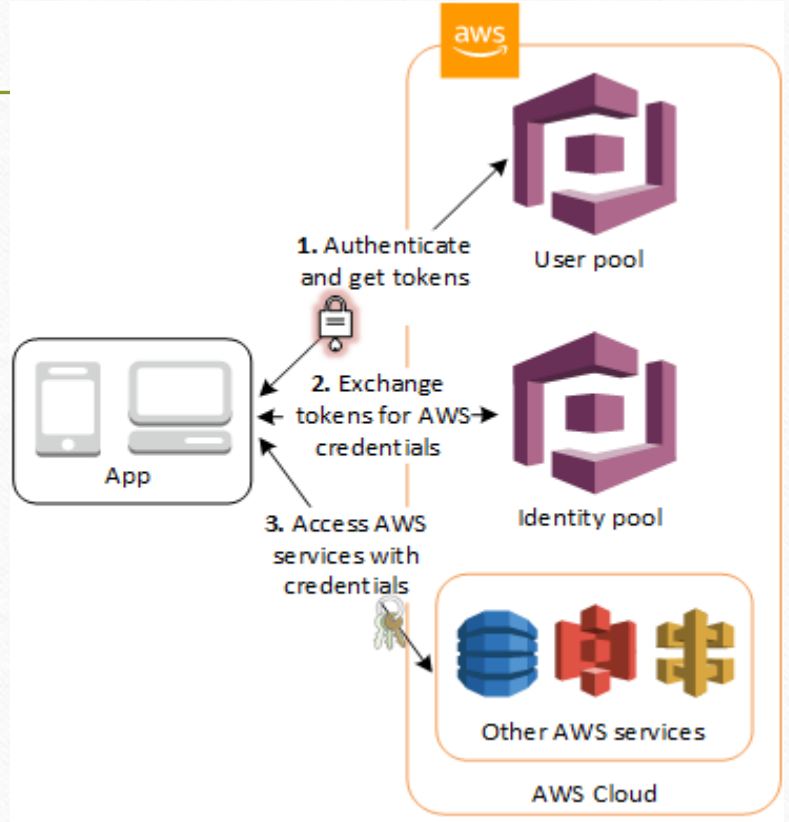
AI APPLICATIONS IN CYBERSECURITY: REAL LIFE EXAMPLES

- **AI-powered threat detection**

- There is a need to improve its cybersecurity processes and tools in organizations.

- The company looked to Cognito, Vectra's AI-based threat detection and response platform. Cognito collects and stores network metadata and enriches it with unique security insights. It uses this metadata along with machine learning techniques to detect and prioritize attacks in real-time.

- Cognito helped ED&F Man Holdings to detect and block multiple man-in-the-middle attacks, and halt a crypto mining scheme in Asia. Moreover, Cognito found command-and-control malware that had been hiding for several years.



AI APPLICATIONS IN CYBERSECURITY: REAL LIFE EXAMPLES

- **Detection of sophisticated cyber-attacks**
- Energy Saving Trust is an organization that is striving to reduce carbon emissions in the U.K. by 80 per cent by 2050. The company was looking for innovative cyber security technology to strengthen its overall cyber defence strategy. This includes defending the company's critical assets, including intellectual property and sensitive client data from sophisticated cyber-attacks.
- After careful evaluation, the company decided to focus on Darktrace's Enterprise Immune System. Darktrace's platform is based on machine learning technology. The platform models the behaviours of every device, user, and network to learn specific patterns. Darktrace automatically identifies any anomalous behaviour and alerts the company in real-time.
- Energy Saving Trust was able to detect numerous anomalous activities as soon as they occurred and alert the security team to carry out further investigations while mitigating any risk posed before real damage is done.

AI APPLICATIONS IN CYBERSECURITY: REAL LIFE EXAMPLES

- **Reducing Threat Response Time**
- A global bank faced sophisticated cyber threats and advanced attacks. The bank needed to improve its threat detection and response. The existing solution could not effectively detect and mitigate new generations of threats.
- The bank's security team deployed Paladon's AI-based Managed Detection and Response Service (MDR) service. Paladon's threat hunting service is based on data science and machine learning capabilities.
- The bank's threat detection and response capabilities for advanced attacks were enhanced. This includes data exfiltration, advanced targeted attacks, ransomware, malware, zero-day attacks, social engineering, and encrypted attacks.

DRAWBACKS AND LIMITATIONS OF USING AI FOR CYBERSECURITY

- AI technology presents some limitations that prevent it from becoming a mainstream security tool.
- **Data sets**—security companies need to use many different data sets of anomalies and malware codes to train the AI system. Getting accurate data sets can require a lot of resources, and time which some companies cannot afford.
- **Hackers also use AI**—to improve and enhance their malware. AI-based malware can be extremely dangerous because it can develop more advanced attacks by learning from existing AI tools.
- **Neural fuzzing**—is used to detect software vulnerabilities by testing large amounts of random input data. A threat actor can combine neural fuzzing with neural networks to gather information about a target software or system and learn its weaknesses.
- **Resources**—organizations need lots of resources including data, memory, and computing power.

THANK YOU