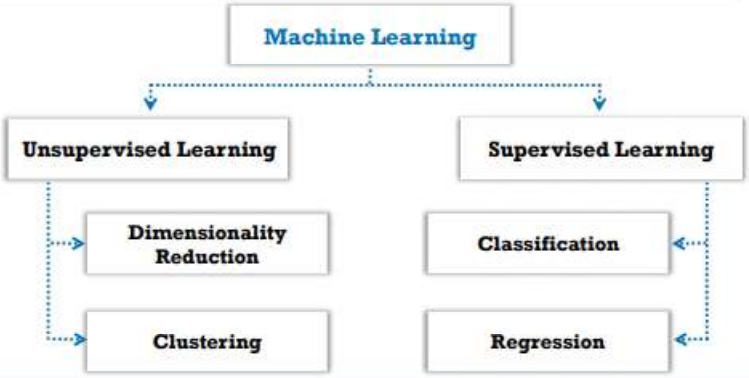
Role of AI and ML in Cyber Security

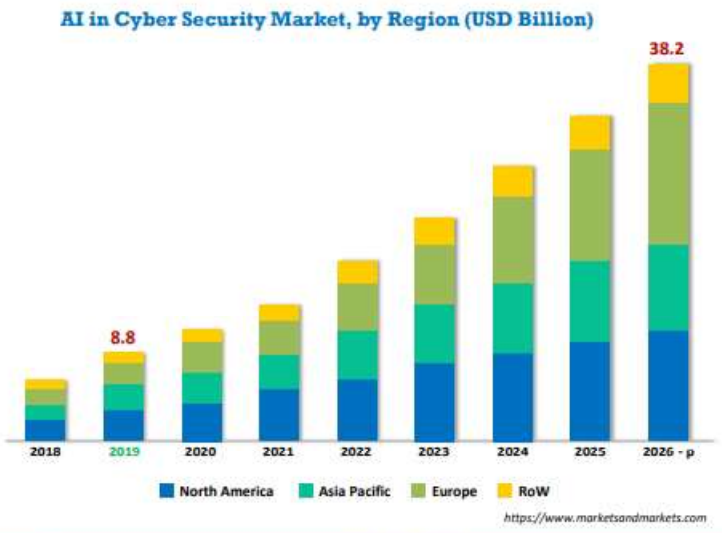
- Machine learning (ML) and artificial intelligence (AI) are now vastly used across various industries and applications due to the **increase in computing power, data collection,** and **storage capabilities**
- ML is an **unsupervised self-learning system** that is used to define what the normal network looks like, along with its devices, and then to backtrack and **report any deviations or anomalies** in real-time
- AI and ML in cyber security helps in **identifying new exploits and weaknesses**, which can then be easily analyzed to mitigate further attacks

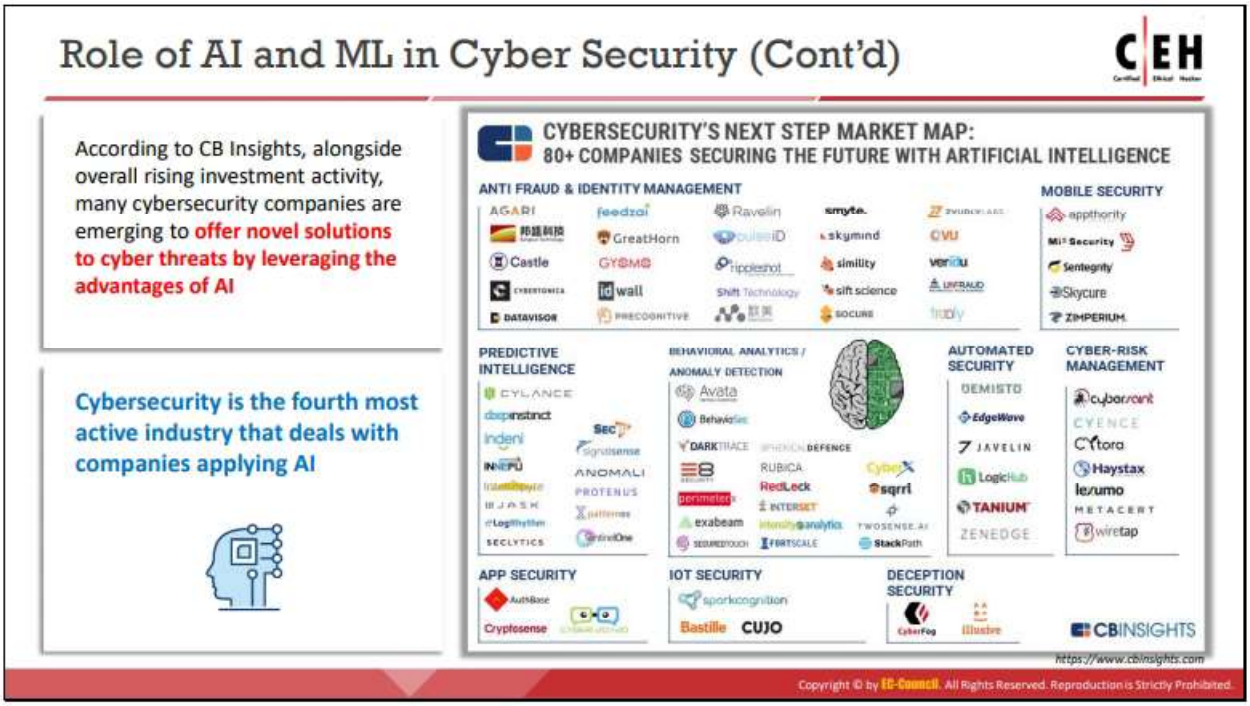
- ML classification techniques:
  - Supervised learning makes use of algorithms that input a **set of labeled training data**, with the aim of learning the differences between the labels
  - Unsupervised learning makes use of algorithms that input **unlabeled training data**, with the aim of deducing all categories by itself



Role of AI and ML in Cyber Security (Cont'd)

- **The cyber security market is set to exceed $300 billion by 2024, and the AI-related cyber security market is predicted to reach a value of $38.2 billion by 2026**





Role of AI and ML in Cyber Security

Machine learning (ML) and Artificial Intelligence (AI) are now popularly used across various industries and applications due to the increase in computing power, data collection, and storage capabilities.

Along with technological advancements in AI, such as self-driving cars, language translators, and big data, there is also a rise in threats such as ransomware, botnets, malware, and phishing. Using AI and ML in cybersecurity helps to identify new exploits and weaknesses, which can be easily analyzed to mitigate further attacks. It reduces the pressure on security professionals and alerts them whenever an action is needed.

What are AI and ML?

Artificial Intelligence is the only solution to defend networks against the various attacks that an antivirus scan cannot detect. A huge amount of collected data is fed into the AI, which processes and analyzes it to understand its details and trends.

ML is a branch of artificial intelligence (AI) that gives the systems the ability to self-learn without any explicit programs. This self-learning system is used to define what the normal network, along with its devices, looks like, and then uses this to backtrack and report any deviations or anomalies in real-time.

There are two types of ML classification techniques:

- **Supervised Learning**

  Supervised learning uses algorithms that input a set of labeled training data to attempt to learn the differences between the given labels. Supervised learning is further divided into two subcategories, namely, classification and regression. Classification includes

completely divided classes. Its main task is to define the test sample to identify its class. Regression is used when data classes are not separated, such as when the data is continuous.

- **Unsupervised Learning**

  Unsupervised learning makes use of algorithms that input unlabeled training data to attempt to deduce all the categories without guidance. Unsupervised learning is further divided into two subcategories, namely, clustering and dimensionality reduction. Clustering divides the data into clusters based on their similarities, regardless of class information. Dimensionality reduction is the process of reducing the dimensions (attributes) of data.

Why AI and ML?

Source: *https://www.gartner.com*, *https://www.marketsandmarkets.com*

The security threat landscape continues to evolve not just in scale, but, more importantly, in sophistication. Despite a range of advancements in the industry to safeguard against increasingly bold and intricate threats, organizations have struggled to keep pace with the technologies and techniques employed by attackers.

As companies continue to increase their digital footprints, "identify and diagnose" capabilities are not enough to remediate against this growing fundamental business challenge for organizations of all shapes and sizes. The development of advanced security analytics is an important consideration for organizations looking to implement machine learning to defend against an array of internal and external security threats.

The cyber security market is set to exceed $300 billion by 2024, and the AI-related cyber security market is predicted to reach a value of $38.2 billion by 2026.

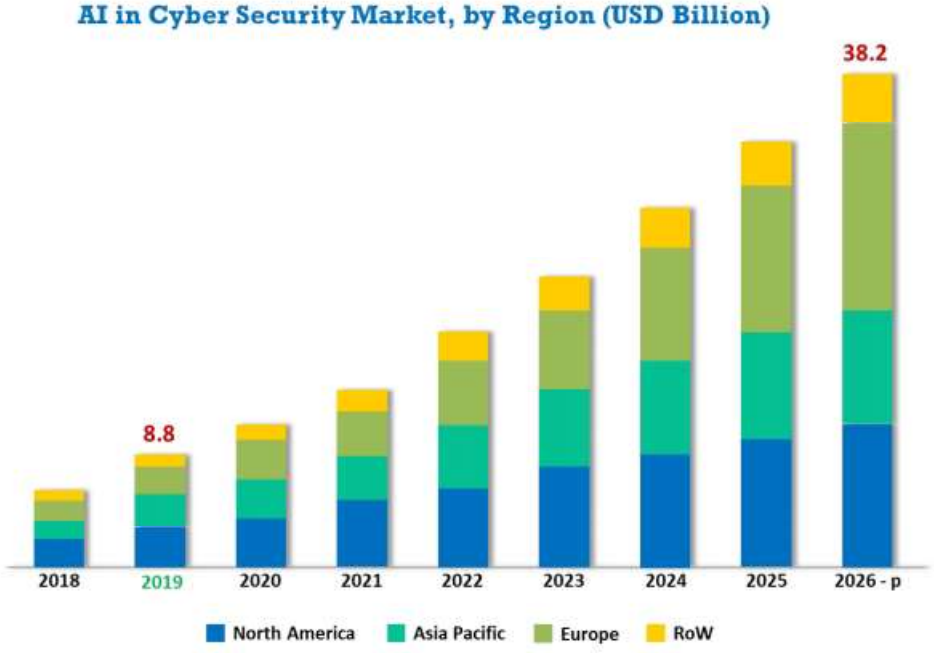


Figure 1.5: AI in Cyber Security Market

AI and ML Application Areas

Source: *https://www.cbinsights.com*

According to CB Insights, alongside overall rising investment activity, many cybersecurity companies are emerging to offer novel solutions to cyber threats by leveraging the advantages of artificial intelligence (AI).

According to CB Insights' AI Deals Tracker, cybersecurity is the fourth most active industry for deals to companies applying AI. As per CB Insights' data, there are over 80 private companies in cybersecurity that are using AI, categorized into the nine main areas in which they operate:

- Anti-fraud and identity management
- Mobile security
- Predictive intelligence
- Behavioral analytics and anomaly detection
- Automated security
- Cyber-risk management
- App security
- IoT security
- Deception security

Figure 1.6: Companies using Artificial Intelligence

How Do AI and ML Prevent Cyber Attacks?

Artificial Intelligence (AI), and with it, Machine Learning (ML), is an emerging technology in the field of cybersecurity. It is widely adopted by largescale industries such as automation, IT services, manufacturing, production, and finance. AI plays a crucial role in detecting imminent cyber threats by incorporating machine learning as a subset.

Following are different ways that AI and ML safeguard industries from cybersecurity attacks:

- **Password Protection and Authentication**

  Password credentials play a critical role in preventing illegitimate access to the organization's or user's data. If credentials are compromised, the reputation of the organization or person could be damaged. Sometimes, traditional face detection and other biometric security measures can also be vulnerable to these credential breaches. Programmers use AI to improve biometric validations and face recognition to thwart such attacks. AI provides the latest models for recognizing an individual's face by tracking key correlations and patterns.

- **Phishing Detection and Prevention**

  Phishing is a common method attackers employ to send their payloads via emails. The majority of users cannot figure out which received emails have a malicious attachment or payload. In this case, AI and ML could play a pivotal role in identifying and preventing such phishing attacks. They can scan and identify phishing emails much faster than a human being can. They can also quickly differentiate malicious websites from legitimate websites.

- **Threat Detection**

  Machine learning assists companies in detecting cyber-attacks before systems are compromised. Being a part of AI, machine learning constantly keeps admins notified of imminent cyber threats by carrying out logical data analysis. ML allows systems to run its algorithms upon the data being received, then performs deep learning on the and comprehends the advancements required to ensure the safety of the information systems.

- **Vulnerability Management**

  AI and ML-based systems never allow vulnerability to exist for long; they dynamically scan for all types of vulnerabilities and alert the admins before the system is exploited. They can also provide the attacker's information and the patterns used to perform the attack. These AI- and ML-based systems can also forecast how and when a vulnerability exploitation might occur.

- **Behavioral Analytics**

  Another notable security improvement by artificial intelligence is "Behavioral Analytics." Attackers who have stolen the credentials of a legitimate user can perform malicious activities on the organization's network; such attempts are difficult to detect and thwart. Here, AI with ML generates specific user patterns based on their regular usage. AI software instantly alerts the admin if it detects any suspicious activity or deviation in regular usage.

- **Network Security**

  Two significant factors of network security are generating comprehensive security policies and mapping an enterprise's network topology. Unfortunately, both of these factors are time-consuming. Therefore, administrators are adopting AI to enhance this operation; it can carry out the network traffic analysis and propose efficient security policies by default.

- **AI-based Antivirus**

  Traditional antivirus tools perform file scanning on the organization's networks to check if any signatures match those of known viruses or malware. The issue with this is that antivirus tools must be updated when the user wants to scan for new malware or viruses. Updating is time-consuming, and new deployment often takes a certain amount of time. To overcome these issues, organizations employ AI-based antiviruses, which use anomaly detection to understand programs' behavior. AI-based antivirus detects suspicious program behavior instead of matching signatures for viruses.

- **Fraud Detection**

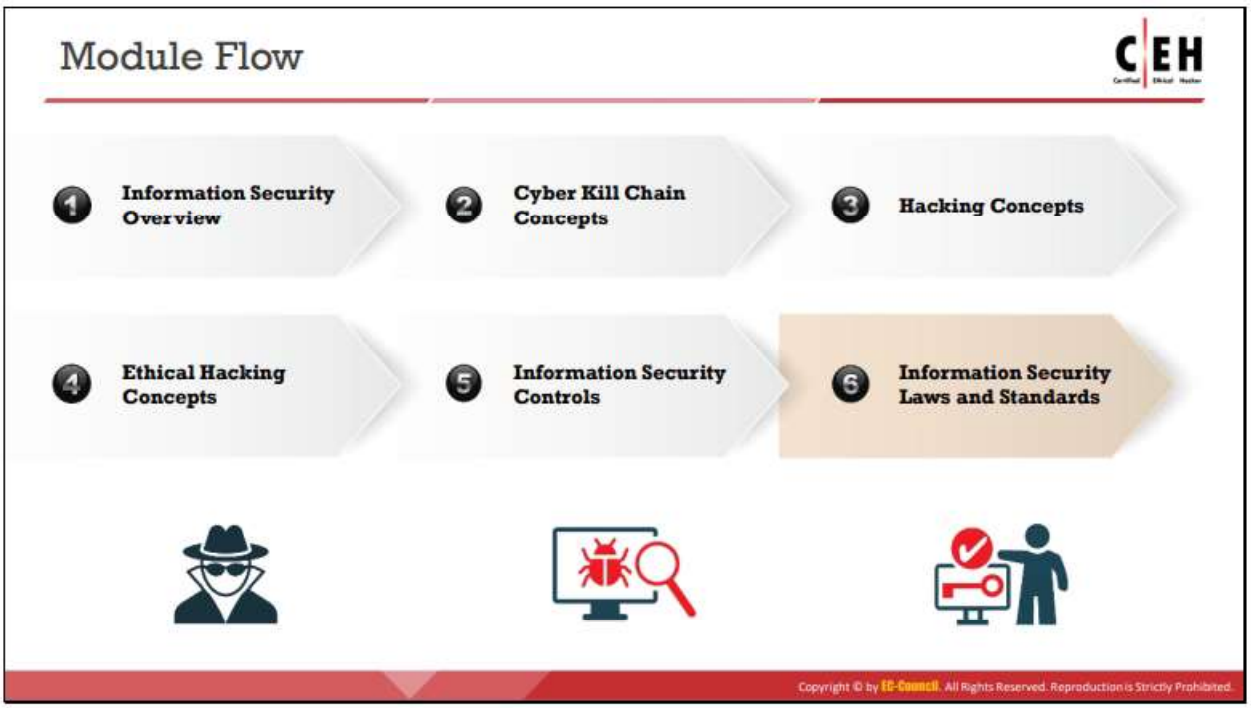
  AI and ML algorithms carry out anomaly detection to identify payment inconsistencies and fraudulent transactions. They also perform automated pattern discovery across different transactions. ML can easily differentiate between authentic and illegitimate transactions and blocks fraudulent transactions.

- **Botnet Detection**

  Botnets can bypass the Instruction Detection System (IDS) by leveraging its ineffectiveness in matching signatures. Botnets can be embedded using a highly sophisticated code that makes them untraceable by traditional IDS implementations. Hence, security professionals use AI and ML algorithms that alert about the suspicious behavior of a network and detect unauthorized intrusions.

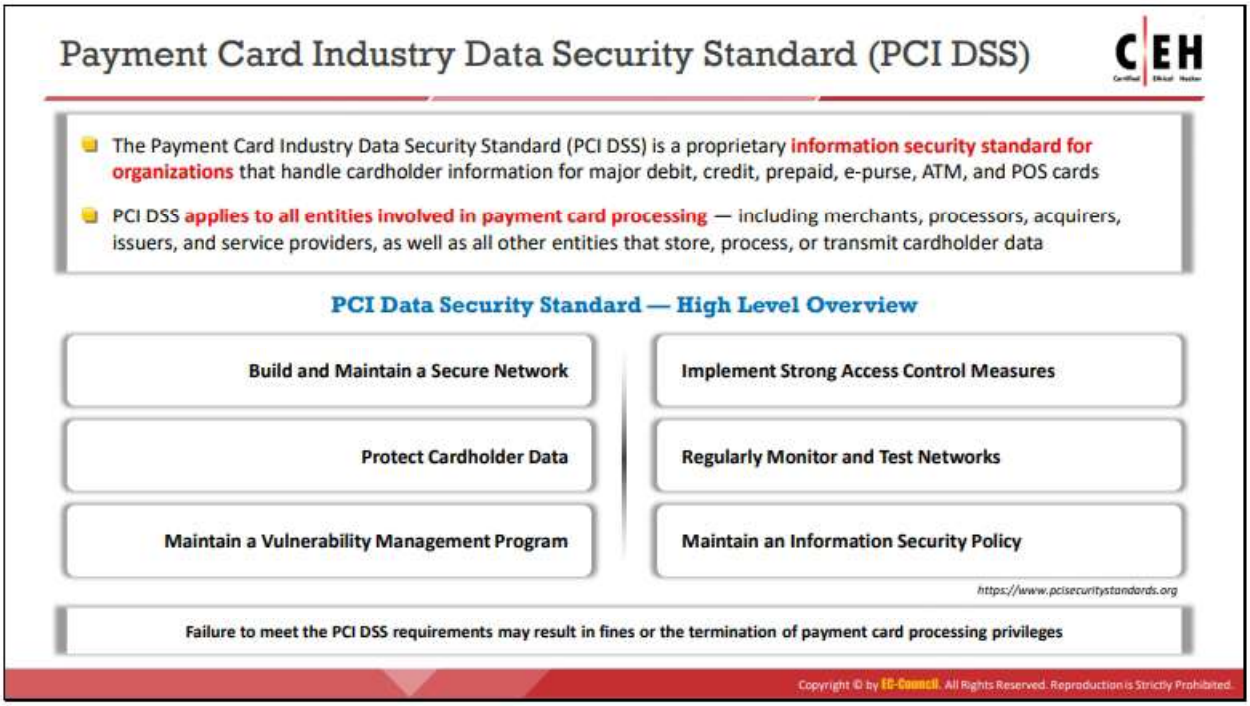
- **AI to Combat AI Threats**

  Attackers can also leverage AI technology to make their way into an organization's network; such cyber threats must be detected immediately. AI software can detect such imminent AI-augmented attacks before the network is compromised.



Information Security Laws and Standards

Laws are a system of rules and guidelines that are enforced by a particular country or community to govern behavior. A Standard is a "document established by consensus and approved by a recognized body that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context." This section deals with the various laws and standards dealing with information security in different countries.



Payment Card Industry Data Security Standard (PCI DSS)

Source: *https://www.pcisecuritystandards.org*

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. This standard offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information. PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data. The Payment Card Industry (PCI) Security Standards Council has developed and maintains a high-level overview of PCI DSS requirements.

PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network	▪ Install and maintain a firewall configuration to protect cardholder data ▪ Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	▪ Protect stored cardholder data ▪ Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	▪ Use and regularly update anti-virus software or programs ▪ Develop and maintain secure systems and applications
Implement Strong Access Control Measures	▪ Restrict access to cardholder data by business need to know ▪ Assign a unique ID to each person with computer access ▪ Restrict physical access to cardholder data
Regularly Monitor and Test Networks	▪ Track and monitor all access to network resources and cardholder data ▪ Regularly test security systems and processes
Maintain an Information Security Policy	▪ Maintain a policy that addresses information security for all personnel

Table 1.3: Table Showing the PCI Data Security Standard—High-Level Overview

Failure to meet PCI DSS requirements may result in fines or the termination of payment-card processing privileges.