

Protecting Against IoT and AI Attacks

Content

- IoT Attacks and Defense
- The Rise of Intelligent Machines

IoT Attacks and Defense

- Case Study
- IoT and IoT Devices
- Smart Homes
- Smart Cities
- IoT Best Practices



Case Study

Case Study

<https://www.businesswire.com/news/home/20221129005177/en/Healthcare-Under-Cyberattack-Unprotected-Medical-IoT-Devices-Threaten-Patient-Care>

Case Study

<https://www.iottechnews.com/news/2022/dec/21/swatters-ring-cams-stream-victims-taunt-police/>

Case Study

<https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>



THANK YOU



IoT and IoT Devices

Internet of Things (IoT)

The internet of things, or IoT, is an interconnected network of computing devices, mechanical and digital machines, objects, animals, or people who are given unique identifiers (UIDs) and the capacity to transfer data over a network without the need for human-to-human or human-to-computer interaction.

Internet of Things (IoT)

The term "thing" refers to any natural or artificial object that can be given an Internet Protocol (IP) address and has the ability to transfer data over a network, including people with implanted heart monitors, farm animals with biochip transponders, cars with built-in tire pressure monitors, and other examples.

Internet of Things (IoT)

The number of IoT devices that are connected has increased significantly, and for the foreseeable future is predicted to increase year over year. There are approximately 13.15 billion connected IoT devices, based on the most recent data.

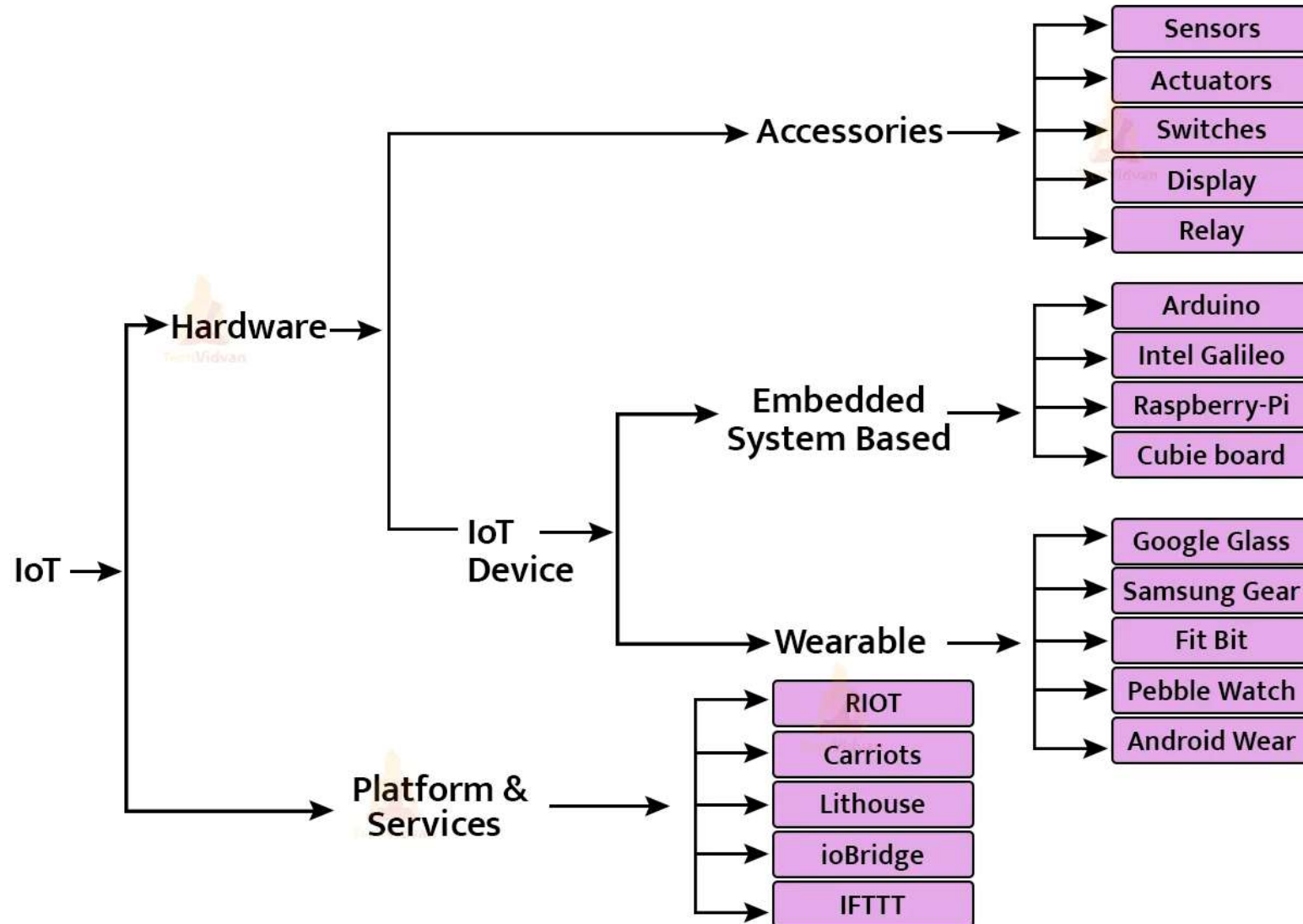


The IoT market is currently worth approximately \$800 billion


IoT Devices

Internet of Things devices are unconventional devices that are able to connect to a network and exchange data. The Internet of Things (IoT) expands connectivity to the Internet beyond conventional devices like smartphones, laptops, tablets, and desktops. Because these things are embedded with technology, we can communicate and interact with them across networks, and they can be remotely monitored and controlled.

IoT Devices and Technologies



IoT Devices



01 IoT smart objects


02 Amazon Echo

03 LG SmartThinQ

04 Smart TV

05 Ecobee Smart Thermostat

06 Amazon Smart oven



The diagram illustrates a central laptop connected via dotted lines to six circular icons representing different IoT applications: a heart with a pulse line (healthcare), a shopping cart (e-commerce), a credit card (finance), a stack of coins (finance), an envelope (communication), and a shopping cart (e-commerce).

Properties of IoT Devices

- **Sense:** The devices that sense their surrounding environment in the form of temperature, movement, the appearance of things, etc.
- **Send and receive data:** IoT devices are able to send and receive data over the network connection.
- **Analyze:** The devices can analyse the data received from the other device over the internet networks.
- **Controlled:** IoT devices may control from some endpoint also. Otherwise, the IoT devices communicate with each other endlessly, leading to system failure.



THANK YOU



Smart Homes

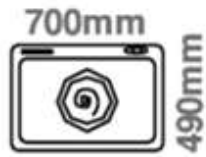
Smart Homes

A smart home is a convenient setup in which appliances and devices may be automatically controlled remotely using a mobile or networked device from anywhere with an internet connection. Devices in a smart home are interconnected via the internet, allowing the user to remotely control features such as home security, heating, lighting, and a home theatre.

Smart Home



Camera



Washing Machine



Refrigerator
or



Light



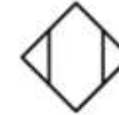
Smoke Alarm



Smart House



Smart TV



Motion Sensor



Thermostat



Moisture Sensor



Lock



Open/Close Sensor



Doorbells

Smart Home Device Attacks

Data Breach and Identity theft

Insecure IoT devices generate data and provide cyber attackers with ample space to target personal information. This could potentially end up in identity theft and fraudulent transactions.

Device hijacking and Spoofing

Smart devices can be hijacked, giving attackers complete control. The attackers can modify the device, spoof communication between two ends, and take control of other devices, or perhaps the entire network.

Smart Home Device Attacks

Distributed Denial of Service (DDoS)

The device or network resource goes unavailable to its intended users by temporarily or indefinitely disrupting the services.

Phlashing:

The device is ruthlessly damaged by such attacks to the point where it must be replaced.

Securing Smart Home Devices After Purchase

Use Strong passwords

Ensure routers and all devices have strong passwords. Hackers frequently use retained default passwords as entry points.

Guest Networks

When possible, use the guest network to connect smart home devices. This can assist in separating the devices from the sensitive data stored on laptops or phones. Even if cybercriminals infiltrate one of the IoT devices, they will not be able to breach the main network and compromise the PCs and smartphones that are connected to it.

Securing Smart Home Devices After Purchase

Two-factor authentication

Enabling two-factor authentication, which needs additional verification via a mobile or authenticator app, significantly decreases hackers' ability to modify devices.

Highest Level Encryption

Use the highest-level encryption (WPA3) on the router to ensure secure communication.

Securing Smart Home Devices After Purchase

Firewalls

Using firewalls is one of the famous ways to secure smart home devices. A firewall enables the user to see potential attacks and manage the security level of individual connected devices. Firewalls send notifications to the host when any abnormality in the network or devices is detected.

You can leverage the built-in firewall feature of your home router or get a dedicated firewall for your smart home.

Smart Home Security





THANK YOU



Smart Cities

IoT and the Smart City

Smart cities use IoT devices such as connected sensors, lights, and meters to collect and analyze data. The cities then use this data to improve infrastructure, public utilities and services, and more.

IoT forms the technical backbone of every smart city in the world, equipping them with the intelligence, interconnection, and instruments needed to improve urban services, optimize resources, and reduce costs. By connecting various devices, systems, and people, IoT can provide real-time data and insights on city operations and infrastructure.

IoT and the Smart City

However, there are some distinct challenges in fully realizing the vision of a smart city – with security being the biggest concern at present. To this end, the interconnectedness of IoT devices creates new vulnerabilities for cyberattacks, data breaches, and unauthorized access.

Smart City Technologies

The foundation of smart cities relies on the utilization of Internet of Things (IoT) devices and networks. These devices, in combination with software solutions, user interfaces, and communication networks, enable and enhance the functioning and efficiency of smart cities.



Smart Cities: Threat and Countermeasures

Around the world, smart cities have deployed billions of connected 'things'. The growth of the Internet of Things (IoT) presents a variety of vulnerabilities that cybercriminals and other bad actors can take advantage of. Smart cities are intended to boost productivity and efficiency, but if cyber security is not taken seriously, they could pose significant risks to both citizens and the government. There are untold numbers of methods and potential vulnerabilities.

Smart Cities: Threats

Data and identity theft

Data generated by unprotected smart city infrastructure such as parking garages, EV charging stations and surveillance feeds provide cyber attackers with an ample amount of targeted personal information that can potentially be exploited for fraudulent transactions and identity theft.

Man-in-the-middle

An attacker breaches, disrupts or spoofs communications between two systems. For example, a man-in-the-middle attack on a smart valve in a wastewater system may be exploited to produce a biohazard leak.

Smart Cities: Threats

Device hijacking

The attacker hijacks and effectively assumes control of a device. These attacks can be difficult to detect because in many cases, the attacker does not alter the basic functionality of the device. In the context of a smart city, a cyber-criminal could exploit hijacked smart meters to launch ransomware attacks on Energy Management Systems (EMS) or stealthily siphon energy from a municipality.

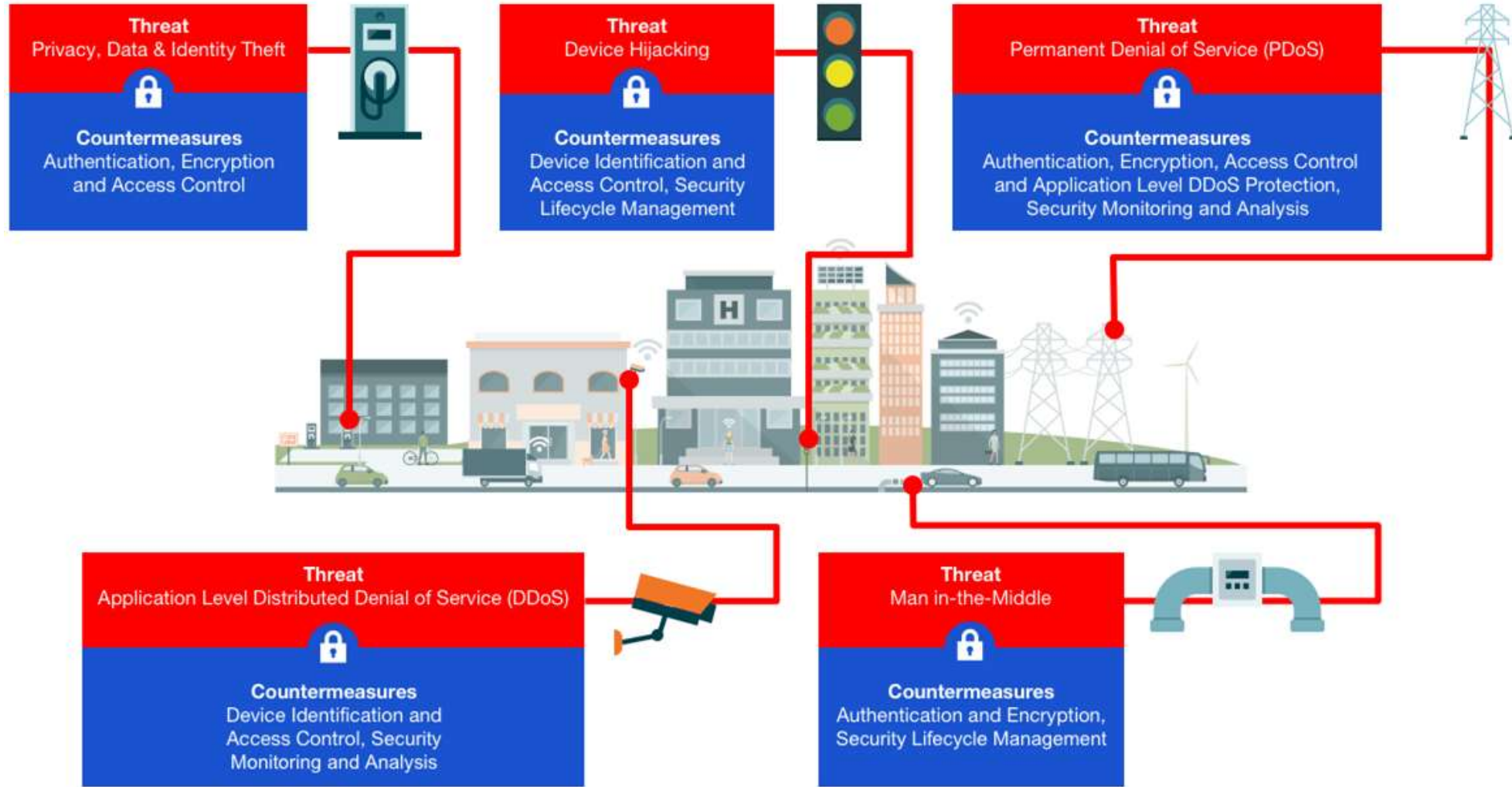
Permanent Denial of Service (PDoS):

Permanent denial- of-service attacks (PDoS), also known loosely as phlashing, is an attack that damages the device so badly that it requires replacement or reinstallation of hardware. In a smart city scenario, a hijacked parking meter could also fall victim to sabotage and would have to be replaced.

Smart Cities: Threats

Distributed Denial of Service (DDoS)

A denial-of-service (DoS) attack attempts to make a machine or network resource unavailable to its intended users by disrupting the services of a host connected to the Internet, either temporarily or permanently. This is usually accomplished by flooding the target with unnecessary requests in order to prevent legitimate requests from being fulfilled. In the case of a distributed denial-of-service (DDoS) attack, the incoming traffic flooding a target comes from multiple sources, making it difficult to stop the cyber offensive by blocking a single source. A variety of smart city equipment, such as parking meters, can be compromised and made to join a botnet programmed to overwhelm a system by requesting service at the same time.





THANK YOU



IoT Best Practices

IoT Best Practices

1. Track and manage your devices.
2. Update your devices and apply patches regularly.
3. Update passwords and credentials.
4. Use up-to-date encryption protocols.
5. Conduct penetration testing or evaluation.
6. Understand your endpoints.
7. Segment your network.
8. Use multi-factor authentication.

Topic Activity

<https://www.businesswire.com/news/home/20221129005177/en/Healthcare-Under-Cyberattack-Unprotected-Medical-IoT-Devices-Threaten-Patient-Care>



THANK YOU



THE RISE OF INTELLIGENT MACHINES

Content

What is AI?

Risks Associated with AI

Protecting Yourself from AI Risks

Safe Use of AI Software

ChatGPT



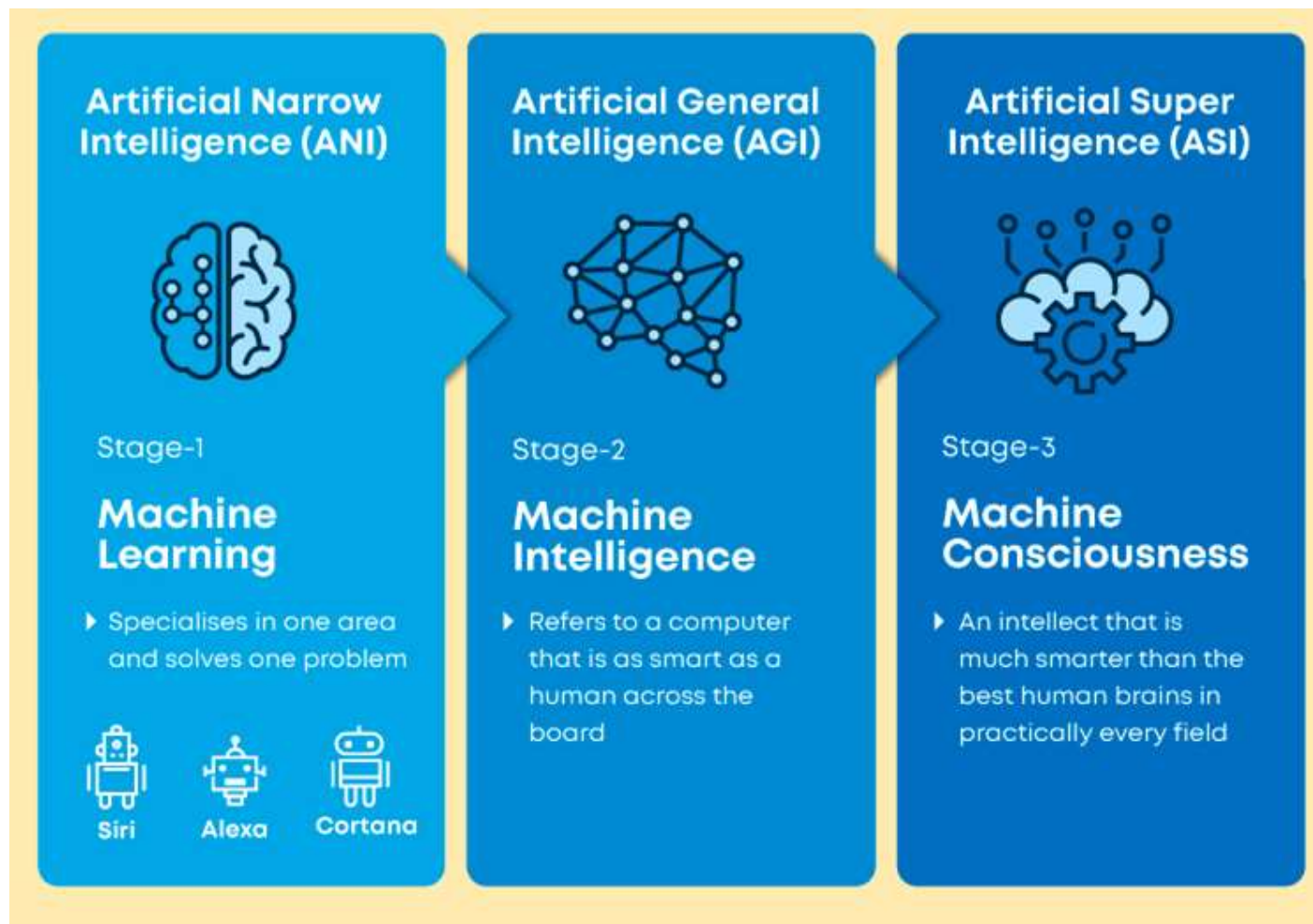
What is AI?

Artificial Intelligence

Machines can learn from experience, adapt to new inputs, and execute human-like jobs because of artificial intelligence (AI). Most AI examples you hear about today rely largely on deep learning and natural language processing, from chess-playing computers to self-driving cars.

AI uses data to automate repetitive learning and discoveries. AI performs regular, high-volume automated tasks rather than automating manual ones. And it does so consistently and without exhaustion. Of course, humans are still required to configure the system and ask the appropriate questions.

3 Types of Artificial Intelligence



Machine Learning

Machine learning is an artificial intelligence application that employs statistical approaches that enable computers to learn and make decisions without being explicitly programmed. It is based on the idea that computers can learn from data, recognize patterns, and make decisions with little help from humans.

It is a subset of AI. It is the study of how to make machines more human-like in their behaviour and decisions by allowing them to learn and generate their own programs. This is accomplished with as little human intervention as possible, i.e. no explicit programming. The learning process is automated and enhanced over time depending on the experiences of the machines.

Deep Learning

Deep learning is a branch of machine learning that trains a computer to perform tasks similar to humans, like speech recognition, image recognition, and prediction making. It strengthens the capacity to categorize, identify, detect, and characterize utilizing data. Deep learning is currently popular because of the buzz surrounding artificial intelligence (AI), in part.

Think of common systems like Siri and Cortana. Deep learning is used in part to power these.



THANK YOU



Risks Associated with AI

Risks of AI

Technological risk—data confidentiality

The secrecy of data is the main technological risk. The advent of AI has made it possible to gather, store, and process information on a previously unimaginable scale, making it incredibly simple to identify, examine, and utilize personal data without others' consent. One of the main causes of customer anxiety and mistrust is the possibility of privacy leaks when using AI technologies.

Risks of AI

Technological risk—security

AI algorithms are the variables that optimize the training data, which gives the AI the capacity to provide insights. If an algorithm's parameters are revealed, a third party might be able to reproduce the model, costing the model's owner money and loss of intellectual property. Additionally, if an online hacker were to change the AI algorithm model's settings without authorization, the AI model's performance would suffer and unpleasant outcomes would follow.

Risks of AI

Usage risk—abuse

The possibility of misuse exists even when an AI system is doing its analysis, decision-making, coordination, and other tasks successfully. It is possible for the operator's use purpose, use technique, use range, and other elements to be corrupted or altered with the intention of causing negative impacts. One example is using face recognition to follow people's movements without their consent.

Risks of AI

Usage risk—inaccuracy

The data that an AI system learns from has a significant impact on how well it performs. Even if an AI system is technically sound, it will produce unfavorable results if it is trained on biased, erroneous, or stolen data.

Topic Activity

In your peer learning groups, discuss the possibility of AI rising against the human race.



THANK YOU



Protecting Yourself from AI Risks

How to Protect Yourself from AI Risks

Limit Online Presence: Limit the amount of personal information, images, and voice recordings you share online. Be cautious about the type and amount of data you share on social media, websites, or other online platforms, as this data could be used by AI systems for various purposes.

Use Privacy Settings: Utilize privacy settings on social media and other online platforms to control who can access and use your images and voice recordings. Review and adjust your privacy settings to ensure that your personal data is only visible to the intended audience.

How to Protect Yourself from AI Risks

Read Terms of Service: When using online platforms that involve uploading images or voice recordings, carefully review the terms of service and privacy policies. Understand how your data may be used by the platform and whether they have any rights or permissions to use your content. Understand the consequences of using those social media apps where you put in information and your photo to get a nickname and avatar image – there is almost always a data usage acceptance behind the scenes that you don't know about unless you look carefully

How to Protect Yourself from AI Risks

Be Cautious with Voice Recordings: Be careful while sharing your voice recordings, especially with unproven or new AI services or applications. Be careful of the possible dangers of voice cloning or voice manipulation and refrain from providing private or sensitive information over voice recordings.

Monitor for Misuse: Regularly monitor the internet for any unauthorized use of your images or voice recordings. You can use reverse image search tools or other monitoring techniques to identify any instances of AI-generated content that may be misusing your image or voice.



THANK YOU



Safe Use of AI Software

Common AI Software

- ChatGPT
- Jupyter Notebooks
- Google Cloud AI Platform
- Azure Machine Learning Studio
- Infosys Nia
- Salesforce Einstein
- Chorus.ai
- Observe.AI Software
- DataRobot
- Tractable
- Content DNA Platform

Safe Use of AI Software

- Understand that AI-powered technologies are by no means secure by design.
- Using AI software to generate content is an effective way to produce ideas or overcome small writer's block. However, depending on the text to provide you with the information is risky. Every fact must be double-checked, and the same applies to software code or ChatGPT answers.
- Be mindful of the information you share with AI Software e.g. information that reveal sensitive data such as PII, images, payment card details etc.

Safe Use of AI Software

- Be mindful of the kind of permission you give to AI software applications on your PCs and smartphones
- Protect all data using various protective technologies on different platforms
- Stop, Think, Share

Topic Activity

Examine the Stupidity of AI

<https://www.theguardian.com/technology/2023/mar/16/the-stupidity-of-ai-artificial-intelligence-dall-e-chatgpt>



THANK YOU



ChatGPT



Hi!
How can I help you.

Case Study

ChatGPT Data Breach

<https://securityintelligence.com/articles/chatgpt-confirms-data-breach/>

ChatGPT

OpenAI created ChatGPT, an AI chatbot made public in November 2022. The name "ChatGPT" combines the words "Chat," which refers to the chatbot feature, and "GPT," which is short for generative pre-trained transformer and refers to a particular kind of big language model.

ChatGPT stands apart from other chatbots because of its reinforcement learning from human feedback model, which allows it to produce natural language, to understand when it has made mistakes, and more.

Risks Associated with ChatGPT

Data privacy and confidentiality: Any information entered into ChatGPT, if chat history is not disabled, may become a part of its training dataset. Sensitive, proprietary or confidential information used in prompts may be incorporated into responses for other users

Intellectual property (IP) and copyright risks: A significant amount of internet data, including maybe copyrighted material, was used to train ChatGPT in particular. Therefore, its outputs could potentially breach copyright or intellectual property restrictions. ChatGPT does not include source citations or descriptions of how its output is produced.

Risks Associated with ChatGPT

Fabricated and inaccurate answers: The primary issue that users encounter with ChatGPT is a tendency to give inaccurate information that appears plausible at first glance.

Cyber fraud risks: False information is already being produced at scale by bad actors using ChatGPT, for example, fake reviews.

Consumer protection risks: Businesses who use ChatGPT without disclosing it to customers (for example, by using a chatbot for customer service) face the risk of losing those customers' trust and being accused of unfair business practices by a number of different legal authorities.

ChatGPT Security Best Practices

- Never input personal identification information (PII)
- Turn off the toggle for “Chat History & Training”: Unchecking this option prevents ChatGPT from saving news talks to your history or using them to train models. Conversations that were not saved will be removed from the system within one month.
- Always verify the data you get from an AI tool before using it.
- Stay vigilant against phishing attacks.

ChatGPT Security Best Practices

- Before using a ChatGPT-powered app or any service that uses OpenAI language models, carefully review the platform's privacy policy and data handling policies to learn how the platform stores and uses your chats.
- Use anonymous or pseudonymous accounts. As a result, there will be less chance that your true identity will be linked to chat data.
- To ensure a high level of security while using ChatGPT, be informed of any changes to OpenAI's security measures or privacy policies and adjust how you operate accordingly.



THANK YOU