Université Abdelhamid Mehri – Constantine 2
Faculté des Nouvelles Technologies de l'Information et de la Communication
Département d'Informatique Fondamentale et ses Applications

Artificial Intelligence of Things (AIoT)

2EMME ANNÉE MASTER
SDIA
S1

DR ILHAM KITOUNI

24-25

Chapitre 4- **Security in AIoT**
Part 1

AIoT-syllabus-ang24-25.docx

1. Introduction to Security in AIoT

Context

AIoT combines the Internet of Things (IoT) with artificial intelligence (AI) to enable connected devices to make autonomous decisions in real time.

This improves processes in various sectors, such as healthcare, industry, and home automation.

In industry, BMW uses AIoT to optimize its production through predictive maintenance, reducing unplanned downtime by 80%

1. Introduction to Security in AIoT

Security Issues

Data volume and sensitivity: AIoT devices collect huge amounts of sensitive data (personal, industrial), making them vulnerable to cyberattacks. Increased.

Complexity: The interconnection of thousands of IoT devices with AI systems increases potential attack surfaces.

2. Example of Security in AIoT

Jeep Cherokee hack In 2015, security researchers demonstrated a critical flaw in a Jeep Cherokee vehicle. They managed to remotely take control of the vehicle via its internet-connected entertainment system.

They could not only change the temperature of the cabin, but also influence the vehicle's steering and brakes.

→ The risks associated with IoT devices in the automotive industry and the importance of securing critical AIoT systems, such as self-driving cars[1].

2. Example of Security in AIoT

Taking control of Ring cameras

Ring smart cameras used for home surveillance, were hacked due to users' use of weak or reused passwords.
The hackers were able to access live video feeds and even communicate with the occupants via the built-in microphones.

This incident highlights the importance of using strong, unique passwords for each AIoT device[2].

2. Example of Security in AIoT

Hack of a connected pacemaker (St Jude Medical)

In the medical field, a vulnerability has been discovered in the connected pacemakers manufactured by St Jude Medical.

carried by 40,000 patients in France, are likely to be taken under the control of third parties Attackers could potentially manipulate these devices to send false signals or deplete their batteries, which could have endangered patients' lives.

No incidents were reported before the flaw was corrected by a software update[4].

2. Example of Security in AIoT

Hacking of a connected washing machine in a hospital In 2020,

A connected washing machine in a hospital was hacked to gain access to the facility's computer system.

While the machine itself is not critical, it has served as an entry point to access sensitive patient data.

This incident shows that even connected objects seemingly harmless can become attack vectors if they are not properly secured[2].

2. Example of Security in AIoT

9

DDoS attack by the Mirai Botnet

The Mirai botnet used vulnerable IoT devices (like surveillance cameras and routers) to launch a massive distributed denial-of-service (DDoS) attack in 2016.

This attack temporarily paralyzed major services such as Twitter and Netflix.

The botnet was operating IoT devices with default credentials unamended, emphasizing the importance of password management and security updates in the AIoT networks[3].

3. Top Security Risks in AIoT

1. **IoT Device Vulnerabilities Physical and software attacks**:

IoT devices are often exposed to direct attacks (e.g., hacking a camera or sensor).

Lack of standardization: The diversity of IoT devices and the lack of universal standards make it difficult to manage securely.

3. Top Security Risks in AIoT

2. Network Risks DDoS attacks:

IoT devices can be commandeered to launch distributed denial-of-service (DDoS) attacks, (the case with the Mirai botnet).

Network intrusions: The massive integration of connected objects into networks exposes them to critical flaws.

3. Top Security Risks in AIoT

3. Threats to Data

Data stealing and manipulation: Data collected by sensors can be intercepted or modified if it is not properly encrypted.

Privacy concerns: In AIoT applications such as connected health, personal data is particularly sensitive.

4. Importance of Security in AIoT – Critical Impa

- **Healthcare**: IoT medical devices (e.g., pacemakers, insulin pumps) can be targeted by cyber-attacks that risk patient safety.
  - *Case*: In 2019, FDA reported a flaw in Medtronic insulin pumps, enabling remote control, leading to a recall [5]
- **Transportation**: Smart vehicles and traffic systems rely on secure, real-time data.
  - *Case*: the Jeep Cherokee hack occurred in 2015, led to Fiat Chrysler Automobiles recalling 1.4 million vehicles to address the security flaws [6].
- **Industry**: Smart factories using IoT sensors and actuators can be compromised, leading to production issues.
  - *Case*: Stuxnet worm targeted industrial IoT, damaging nuclear centrifuges in Iran [7].

5. Key Security Challenges in AIoT

1. **Device Diversity**: Varying processing power, protocols, and operating systems complicate unified security.
    1. *Example*: A smart home with devices using different protocols like Zigbee, Wi-Fi, or Bluetooth.
2. **Network Heterogeneity**: AIoT devices operate over diverse networks (e.g., cellular, LoRaWAN, Wi-Fi).
    1. *Example*: Smart city systems with streetlights on LoRaWAN, cameras on 4G/5G, creating complex security needs.
3. **Data Management Complexity**: High volume and sensitivity of AIoT data (e.g., biometric data) demand robust protection.
    1. *Example*: Wearables collecting health data risk privacy if compromised.