



Usage Areas and Opportunities of Artificial Intelligence in Cybersecurity

Dr. Özgür Can TURNA
ozgurcan.turna@istec.com.tr

Enhancing Security in the Digital Era

What is AI and Why Cybersecurity Matters

➤ What is AI?

- Machines mimicking human intelligence (ML, NLP, Deep Learning).

➤ Why Cybersecurity Matters:

- Rising cyber threats (ransomware, phishing, DDoS).

How AI is Transforming Cybersecurity

- Real-time threat detection and response.
- Reduces human error and improves efficiency.
- Key areas: Threat detection, fraud prevention, endpoint protection.

Key Usage Areas of AI in Cybersecurity

- **Threat Detection:** Finds anomalies in network traffic.
- **Fraud Detection:** Flags suspicious transactions.
- **Endpoint Protection:** Secures devices like laptops.
- **Incident Response:** Automates threat responses.

AI-Powered Threat Detection

- AI spots unusual patterns in data.
- Example: Detecting zero-day exploits.
- Case Study: AI stopping a phishing attack.

AI in Fraud Detection and Endpoint Protection

- **Fraud Detection:** AI monitors transactions for fraud (e.g., credit card fraud).
- **Endpoint Protection:** AI-powered antivirus detects malware and ransomware.

An abstract network diagram featuring several grey cylindrical nodes connected by thin grey lines. The nodes are arranged in a non-uniform pattern, with some having multiple connections, suggesting a complex network structure. The background is a dark blue gradient.

Opportunities of AI in Cybersecurity

- **Proactive defense:** Predicts and prevents attacks.
- **Scalability:** Handles large networks.
- **Cost efficiency:** Reduces manual work.
- **Continuous learning:** AI improves over time.

Challenges of AI in Cybersecurity

A wooden balance scale is centered in the background. The left pan holds a blue shield with a white question mark, while the right pan holds a blue padlock. The scale is slightly tilted, with the right pan being lower, suggesting the padlock is heavier. The entire scene is set against a dark, textured background.

- **False positives:** AI may flag harmless activities.
- **Adversarial attacks:** Hackers using AI against systems.
- **Ethical concerns:** Privacy and bias issues.

Future Trends and Ethical Considerations

- **Future Trends:** Autonomous security systems, AI securing IoT, quantum computing.
- **Ethical Considerations:** Balance security and privacy, ensure transparency, avoid bias.

Conclusion and Q&A

- **Recap:** AI is transforming cybersecurity with huge opportunities and challenges.
- **Call to action:** Invest in AI-driven solutions.
- Thank you! Questions?

ISTEC

cyber security

istec.com.tr