Tishk International University
Faculty of Applied Science
Cybersecurity Department

Lecture 11 : Emerging Technologies: AI, IoT, Cloud Computing

CBS221/A: Ethics and Legal Issues in Cybersecurity

Week 12: 21-25/12/2025Instructor:

Prof. Dr. Qaysar Salih Mahdi

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Title & Overview

- **This lecture focuses on how modern emerging technologies—Artificial Intelligence (AI), the Internet of Things (IoT), and Cloud Computing—are reshaping cybersecurity.**
  We will explore both defensive and offensive applications, discuss real-world case studies, and analyze the ethical, legal, and governance implications.
  Emphasize that technological convergence creates both opportunities for innovation and challenges for digital defense.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Learning Objectives

- Bullets:
- Understand AI, IoT, and Cloud integration in security systems
- Identify new vulnerabilities and risk domains
- Apply frameworks for secure design and governance

By the end of this lecture, participants should be able to:

- Explain how AI automates and enhances cyber defense.
- Evaluate risks introduced by IoT's massive connectivity.
- Analyze cloud-based security models and shared responsibilities.
- Design practical controls for hybrid AI-IoT-cloud environments. These objectives align with cybersecurity governance, digital resilience, and sustainable technology use.

Introduction: Emerging Technologies Landscape

Bullets:

Definitions: AI, IoT, Cloud Computing

Technology convergence

Impact on cybersecurity ecosystems

Lecture Notes:
Define:

AI: Systems capable of learning, reasoning, and adapting (e.g., ML, DL).

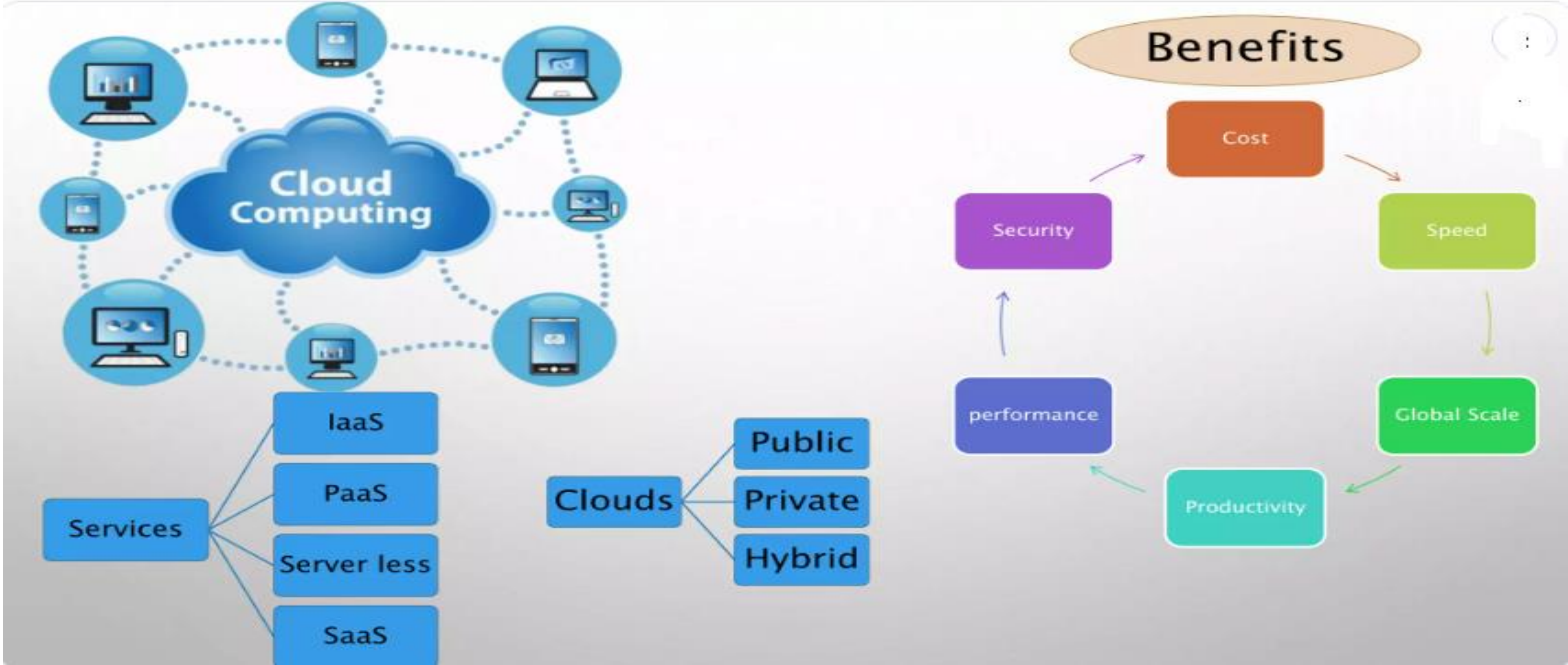
IoT: A network of interconnected sensors and devices generating vast data streams.

Cloud Computing: On-demand scalable resources enabling flexible infrastructure.
Convergence leads to new attack surfaces—AI models hosted in the cloud, IoT devices feeding sensitive data to AI-based analytics.

Currently available emerged technologies

- Artificial Intelligence
- Robotics
- IoT
- 5-G
- Biometrics
- 3D printing
- Cloud Computing
- Big Data

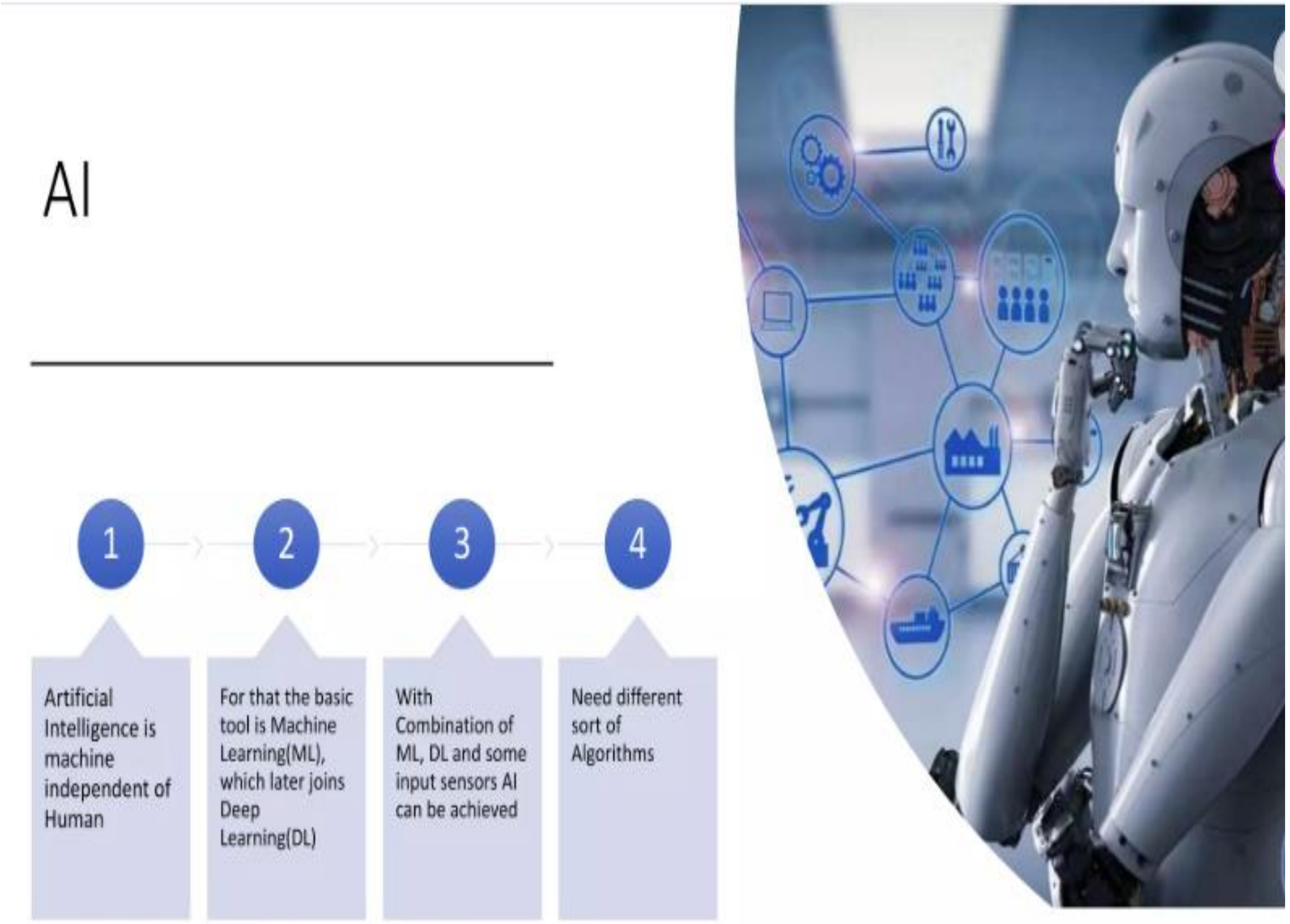
Source: internet


Cloud Computing
Services
IaaS
PaaS
Server less
SaaS
Clouds
Public
Private
Hybrid
Benefits
Cost
Speed
Global Scale
Productivity
performance
Security

Tishk International University
Faculty of Applied Science
Cybersecurity Department

AI in Cybersecurity — Overview

- Bullets:
- AI as a defender and attacker
- Uses: Detection, response, and prediction
- Applications: SOC automation, malware classification
- AI supports anomaly detection, user behavior analytics (UEBA), and threat hunting.
However, adversaries exploit AI for automated phishing, malware generation, and AI-powered social engineering.
AI is dual-edged: it strengthens defenses but can also magnify threats.



Definition
- Combination of technologies and process to protect data and programs from unauthorized access

Importance
- Different bodies such as government, military, corporate, financial...stores, process unprecedented data on computers, for safeguarding such Data

Challenges
- Network security
- Application security
- Endpoint security
- Data security

Machine Learning vs Deep Learning

- Bullets:
- ML: Supervised, Unsupervised, Reinforcement
- DL: Neural networks for feature extraction
- Application comparison
  ML models rely on structured features (e.g., file size, IP reputation), while DL automatically extracts features from raw data (e.g., packet captures, logs). Example: ML may classify phishing URLs, while DL models (CNN/RNN) detect unseen threats.
  Reinforcement learning simulates adaptive attacker–defender behavior.
  Key tradeoff: Interpretability vs accuracy.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

AI-based Threat Intelligence & Detection

SIEM + ML correlation

UEBA and anomaly detection

Automated threat scoring

Modern Security Operations Centers (SOCs) integrate machine learning models into SIEM platforms to prioritize alerts.
AI correlates massive log data, identifying anomalies humans might miss.
Example: Microsoft Defender or Splunk use ML pipelines to detect insider anomalies.
Challenges include data drift, false positives, and model retraining.

Example Problem:

A SOC receives 1 million daily log entries. An ML-based anomaly detector flags a subset as "abnormal." After validation, analysts discover 40 of 50 alerts were true attacks.

Question:

What is the model's precision, and how can it be improved?

Solution:

Precision = True Positives / (True Positives + False Positives)

= 40 / 50 = 0.8 (80%).

To improve:

- Use ensemble models for balanced learning.
- Periodically retrain with updated threat datasets.
- Apply feature selection to reduce noise.

Adversarial ML & Evasion Techniques

- Bullets:
- Evasion and poisoning
- Model inversion and theft
- Countermeasures

Attackers use adversarial samples—inputs slightly modified to mislead models.
Example: Changing few bytes in malware may evade a classifier.
Poisoning attacks corrupt training data, degrading model reliability.
Defense: adversarial training, differential privacy, explainable AI, and layered verification.

Example Scenario:

An antivirus ML model classifies malware using byte sequences.
An attacker modifies the file slightly without changing its behavior, causing the model to misclassify it as benign.

Problem:

Explain the type of adversarial attack and one mitigation technique.

Solution:

- Attack Type: Evasion Attack (adversarial example).
- Mitigation: Use adversarial training, where the model is retrained with crafted adversarial samples to improve robustness.

Additional Example:

If 1% of training data is poisoned (contains mislabeled malware as safe), model accuracy can drop from 95% → 70%.
Solution: Data provenance tracking and outlier detection during preprocessing.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

AI in Malware & Phishing

- **Bullets:**
- **AI-generated phishing emails**
- **ML-driven malware mutation**
- **AI for automated reconnaissance**
- **Lecture Notes:**
  AI can simulate human writing to craft convincing spear-phishing messages (e.g., GPT-based attacks).
  Malware families now use ML polymorphism—they modify behavior dynamically.
  Countermeasures: sandboxing, real-time heuristic monitoring, and behavioral ML filters.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

IoT Overview & Architecture

- **Bullets:**
- **Devices, Gateways, Cloud**
- **Protocols: MQTT, CoAP, HTTP**
- **Lifecycle & constraints**
-

IoT architecture:
- **Perception layer: sensors & devices**
- **Network layer: connectivity (Wi-Fi, LTE, Zigbee)**
- **Application layer: cloud-based analytics IoT security is limited by weak encryption, long lifecycles, and vendor fragmentation.**

Tishk International University
Faculty of Applied Science
Cybersecurity Department

IoT Attack Surfaces & Vulnerabilities

- Bullets:
- Default passwords
- Firmware vulnerabilities
- Lateral network movement
- Lecture Notes:
  Common weaknesses:
- Unchanged factory credentials (Mirai botnet)
- Insecure update mechanisms
- Flat networks allowing pivot attacks
  Highlight: IoT is often an entry point for deeper infrastructure breaches.

Example Problem:

An IoT security camera is connected to a public Wi-Fi network with default credentials. Within hours, it becomes part of a DDoS botnet.

Question:

Identify the attack vector and preventive control.

Solution:

- Attack Vector: Weak authentication (default credentials) and exposed telnet/SSH ports.
- Control: Change default passwords, use firmware-level encryption, and isolate IoT subnet (VLAN).

Case Studies: Real-World IoT Attacks

- Bullets:
- Mirai Botnet (2016)
- Smart Camera Leaks
- Industrial IoT attacks
- Mirai: infected thousands of IoT devices to create DDoS attacks exceeding 1 Tbps.
- Smart Cameras: exposed feeds due to weak APIs.
- Industrial IoT: attacks on SCADA systems threaten critical infrastructure.
  Lesson: simple misconfigurations can trigger global effects.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Risk Management for IoT Deployments

- Bullets:
- Device inventory & segmentation
- Secure boot, attestation
- Lifecycle patching
- Lecture Notes:
  Adopt a risk-driven approach:
- Identify devices, assign criticality.
- Enforce segmentation—IoT devices isolated from core networks.
- Use secure boot and signed firmware.
- Plan for updates and decommissioning.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Cloud Computing Fundamentals

- Bullets:
- Models: IaaS, PaaS, SaaS
- Deployment: Public, Private, Hybrid
- Benefits vs risks
- Lecture Notes:
  Define:
- IaaS: Infrastructure layer (AWS EC2, Azure VMs)
- PaaS: Application platforms (Google App Engine)
- SaaS: Full-service apps (Office 365)
  Risks: multi-tenancy, lack of visibility, and dependency on provider controls.

Cloud Security Models & Controls

- Bullets:
- IAM & Access Policies
- Encryption & Key Management
- Network Isolation
  Emphasize Zero Trust IAM: least privilege, role separation.
  Use KMS for encryption keys.
  Adopt microsegmentation with VPCs, WAFs, and traffic monitoring.
  Encourage continuous auditing using cloud-native tools.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Shared Responsibility Model

- Bullets:
- Cloud provider vs customer duties
- Common misconfigurations
- Case studies
- Provider secures hardware, hypervisors; customer secures OS, apps, and data.
  Breaches often result from misconfigured S3 buckets or overly permissive IAM roles.
  Prevention: infrastructure-as-code scanning and automated compliance tools.

Example Case:

A company hosts sensitive data on AWS S3. Data leak occurs when the S3 bucket is publicly accessible.

Question:

Who is responsible under the shared responsibility model?

Solution:

- **AWS secures infrastructure (hardware, hypervisors).**
- **Customer is responsible for configuration and access management.**

Thus, the organization is accountable for the breach.

Practice Tip:

Always run AWS Config or Azure Security Center scans for misconfigurations.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Cloud Threats & Incident Examples

- Bullets:
- Unified ecosystem
- Cloud AI for IoT telemetry
- Edge AI for low latency
- Lecture Notes:
  Modern architectures blend:
- IoT sensors collecting data →
- Cloud AI analyzing and predicting threats →
- Edge AI executing local responses instantly.
  Challenges: latency, data privacy, synchronization, and model drift

Example:

Ransomware spreads via cloud-synced folders, encrypting local and synced backups.

Problem:

How can cloud resilience mitigate this?

Solution:

- **Enable versioned backups (immutable storage).**
- **Deploy ransomware behavior analytics in the cloud.**
- **Apply multi-factor authentication (MFA) to API access keys.**

Integrating AI, IoT, and Cloud for Security

- Bullets:
- Defense-in-depth
- Zero Trust framework
- AI-assisted response
-

  Combine:
- Defense-in-depth: multiple layers—network, endpoint, cloud.
- Zero Trust: no implicit trust; always verify.
- SOAR + AI: automation for alert triage and containment.
  Key metric: Mean Time to Detect (MTTD) & Respond (MTTR) reduction.

Practical Defense Strategies

- Bullets:
- Defense-in-depth
- Zero Trust framework
- AI-assisted response
- Lecture Notes:
  Combine:
- Defense-in-depth: multiple layers—network, endpoint, cloud.
- Zero Trust: no implicit trust; always verify.
- SOAR + AI: automation for alert triage and containment.
  Key metric: Mean Time to Detect (MTTD) & Respond (MTTR) reduction.

Exercise:

Given a hybrid environment with IoT sensors, AI analytics, and a cloud dashboard:

1. Identify three key risks.
2. Suggest specific countermeasures.

Solution Example:

Risk	Countermeasure
IoT device takeover	Firmware signing + network segmentation
Cloud credential theft	IAM least privilege + MFA
AI model manipulation	Data validation + model explainability

Ethical, Legal & Governance Considerations

- **Bullets:**
- Privacy and transparency
- Legal frameworks
- AI ethics and fairness
- **Lecture Notes:**
  Regulations: **GDPR, ISO 27017, NIST SP 800-207**.
  AI brings ethical challenges: bias, surveillance, and data misuse.
  Promote **accountability, explainability**, and **responsible AI** aligned with cybersecurity governance.

Summary & Takeaways

- Bullets:
- Recap key lessons
- Discussion & Q&A
- Assignments
-

  Reiterate:
- AI: enhances but also threatens security.
- IoT: expands attack surface exponentially.
- Cloud: transforms risk ownership and visibility.
  Assignments:
- Analyze a case study (e.g., Tesla Cloud breach).
- Develop an IoT security checklist.
  Encourage students to discuss “how convergence reshapes defense.”

Discussion & Q&A

- Open floor for questions
- Group discussion: propose a mitigation for a given scenario
- Assign readings and lab tasks
- Discussion Prompt:
- *“In what ways can AI, IoT, and Cloud Computing collaborate to build a self-defending cybersecurity ecosystem?”*
  Encourage students to discuss: automation, anomaly detection, and shared responsibility.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Homework 1: AI Threat Detection Lab

Objective:

Build a simple **machine learning–based anomaly detector** using simulated network data.

Instructions:

1. Download an open dataset (e.g., *CICIDS2017* or *NSL-KDD*).
2. Use Python (Scikit-learn) to train a classifier to detect abnormal connections.
3. Evaluate accuracy, precision, and recall.
4. Write a short reflection (1 page) on how ML could be attacked or misled (adversarial learning).

Expected Learning Outcome:

Students understand **how AI aids in cyber defense** and recognize **its vulnerabilities**.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Homework 2: Cloud Security Configuration Audit

Objective:

Perform a **practical review of cloud security settings** using simulation or cloud lab (AWS Educate / Azure for Students).

Instructions:

1. Create a small **virtual private cloud (VPC)** or sandbox account.
2. Configure IAM users, S3 buckets (or Blob storage), and set access policies.
3. Intentionally create one misconfiguration (e.g., public bucket).
4. Detect and fix it using a security scanner (AWS Config, Cloud Security Posture Management tools).
5. Submit screenshots and a 1-page report describing the risk, fix, and lessons learned.

Expected Learning Outcome:

Students apply **shared responsibility** and **cloud misconfiguration analysis** to practical settings.

Optional Bonus Activity:

IoT Risk Mapping Exercise — Identify 5 IoT devices at home or campus and map their data flow, risks, and defenses. Submit a visual diagram.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

References

Academic Sources

1.Goodfellow, I., Shlens, J., & Szegedy, C. (2020). *Explaining and Harnessing Adversarial Examples*. arXiv:1412.6572.
2.Papernot, N., McDaniel, P., et al. (2021). *Adversarial Machine Learning in Practice*. IEEE Security & Privacy.
3.Alaba, F. A., et al. (2020). *Internet of Things Security: A Survey*. Journal of Network and Computer Applications.
4.Cloud Security Alliance (CSA). (2023). *Security Guidance for Critical Areas of Cloud Computing v5.0*.
5.Zhang, L. & Wang, S. (2022). *AI-Powered Cyber Defense Systems*. Computers & Security Journal.

Professional / Standards

6.NIST SP 800-207. (2023). *Zero Trust Architecture*.
7.ISO/IEC 27017:2021. *Information Security Controls for Cloud Services*.
8.MITRE ATT&CK Framework (2024 update).
9.ENISA. (2024). *Guidelines on Securing AI and Machine Learning*.
10.OWASP IoT Project (2023). *Top 10 IoT Security Issues*.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Thank you for your listening