C 11

DECISION MAKING IN AI AND CYBERSECURITY

Overview, Machine Decision Logic, and Role of Cybersecurity

Robotics and AI Faculty

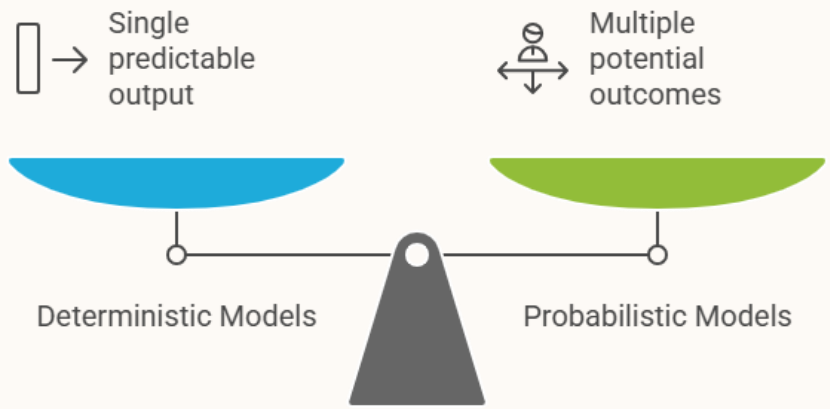
Dr. Saptarshi Jana
saptarshi.jana@techvein.com

OVERVIEW OF DECISION MAKING

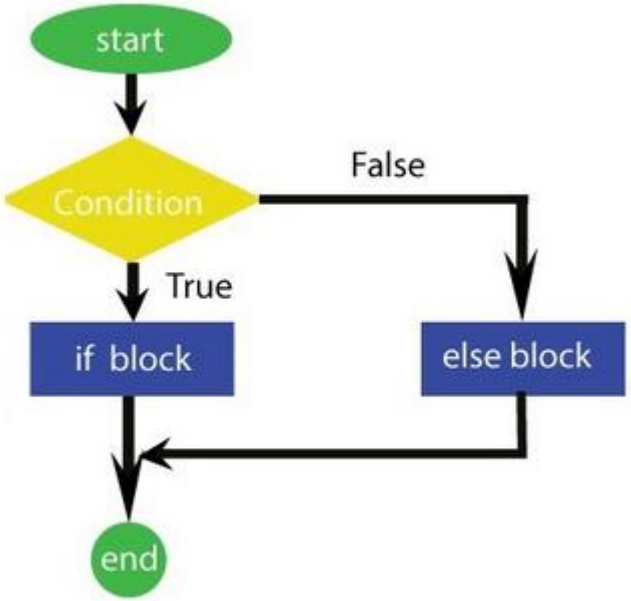
- Decision making is the process of selecting a course of action from multiple alternatives.
- Decision making in humans involves emotions, experiences, and intuition, alongside logic and reasoning.
- In AI, it uses data, logic, and algorithms to choose the optimal solution, ideal for data-driven tasks.

DETERMINISTIC VS PROBABILISTIC MODELS (RECAP)

- **Deterministic Model:** Produces the same output for a given input every time. There is no randomness involved.
  - Example: Newton's laws of motion — if you know the initial conditions, you can predict future states exactly.
- **Probabilistic Model:** Incorporates randomness and uncertainty. Outputs are given as probabilities or distributions.
  - Example: Weather forecasting — even with the same inputs, outcomes are given in terms like "70% chance of rain."



DECISION MAKING IN MACHINES/COMPUTER



Machines rely on algorithms, data analysis, and predefined rules or models, make decisions through logic, data, and algorithms:

- ❑ Rule-Based Systems: If-then logic rules
- ❑ Machine Learning: Learns from data patterns
- ❑ Reinforcement Learning: Learns via rewards and penalties
- ❑ Neural Networks: Deep learning for complex problems

OBJECT CLASSIFICATION

How Humans Classify an Object in an Image (Subjective Decision-Making):

Humans rely on visual perception, experience, intuition, and context to classify objects. This process is often **subjective**, influenced by prior knowledge, cultural background, expectations, and emotions. Two people might interpret the same image differently, especially in ambiguous or unclear scenarios.

How Machines Classify an Object in an Image (Objective Decision-Making):

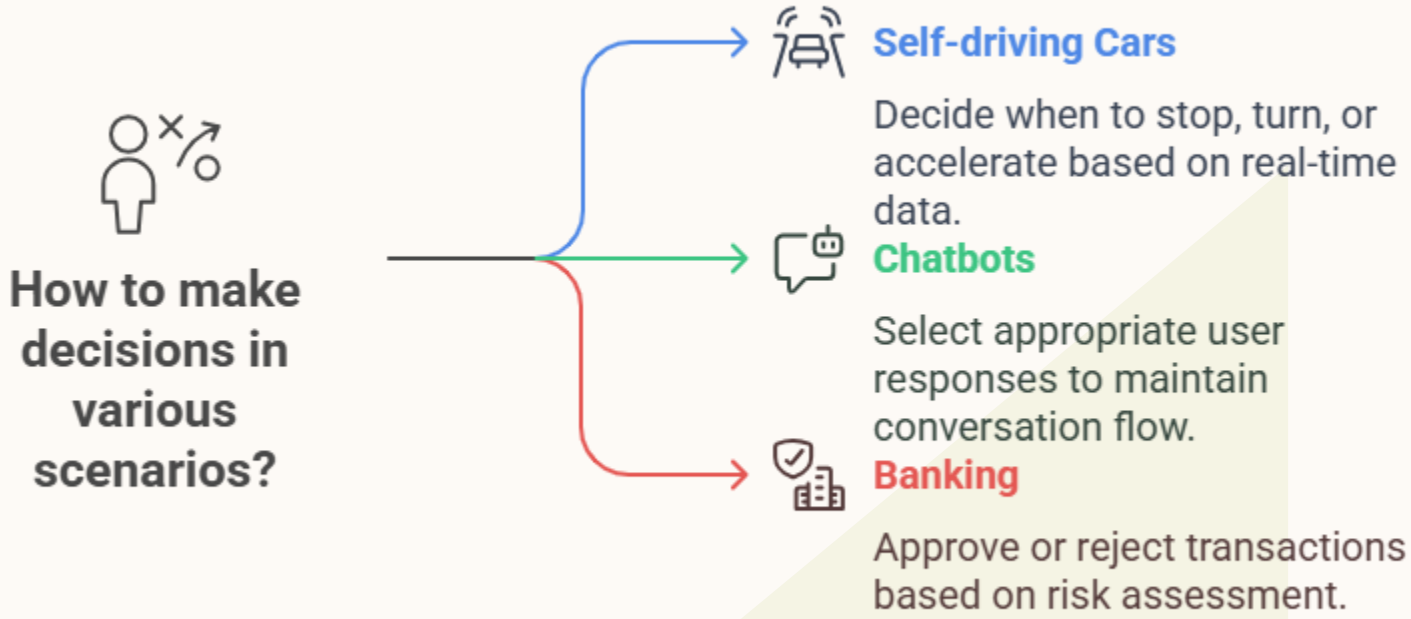
Machines use **objective**, data-driven methods like Convolutional Neural Networks (**CNNs**). The classification depends strictly on learned features from training data (e.g., shape, texture, edges). Given the same input, a trained model will consistently output the same classification, making machine decisions **objective and repeatable**, but dependent on the quality and bias of the training data. The process includes:

- **Image pre-processing** (resizing, normalization),
- **Feature extraction** (edges, shapes, patterns),
- **Classification** using a trained model,
- **Output** as a label with associated probability.

DIFFERENCES BETWEEN HUMAN AND MACHINE DECISION MAKING

Aspect	Human Decision-Making	Machine Decision-Making
Basis	Emotions, intuition, experience, logic	Data, algorithms, logic
Adaptability	Highly adaptive to new, ambiguous, or unfamiliar situations	Limited to trained or programmed scenarios
Speed	Slower, especially for complex or unfamiliar problems	Fast, especially for data-intensive tasks
Consistency	May vary due to mood, fatigue, or bias	Highly consistent and repeatable
Bias and Subjectivity	Susceptible to personal biases and emotions	Can be biased if trained on biased data, but otherwise objective

APPLICATIONS OF AI DECISION MAKING



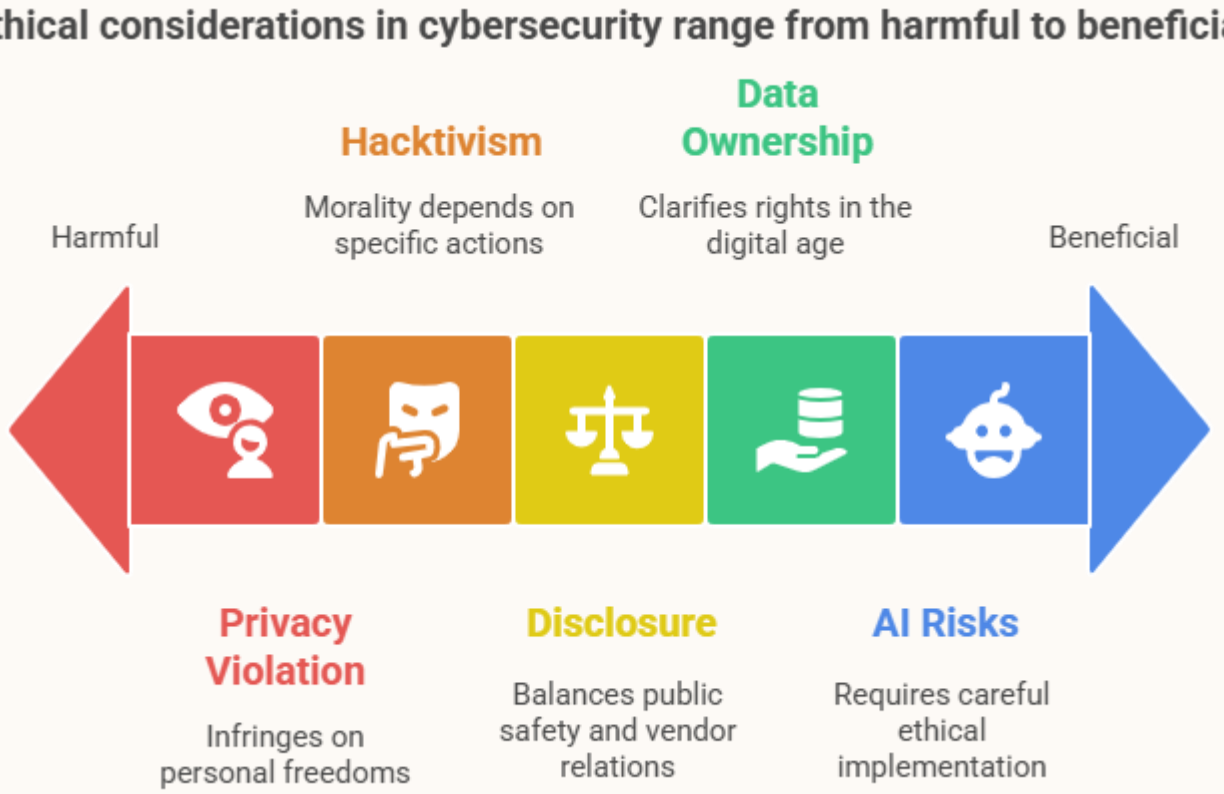
CYBERSECURITY

Cybersecurity refers to the practice of protecting **computers, networks, systems, and data** from digital attacks, unauthorized access, or damage. It includes tools, policies, and practices designed to ensure confidentiality, integrity, and availability of information.

Key Roles of Cybersecurity in AI (Computing):

- **Protecting Data**: Prevents unauthorized access to sensitive personal or business data.
- **System Integrity**: Ensures systems and software are not altered maliciously.
- **Network Security**: Safeguards communication channels and online transactions.
- **User Authentication**: Verifies identity to prevent misuse or impersonation.
- **Business Continuity**: Minimizes downtime and ensures quick recovery after cyberattacks.
- **Regulatory Compliance**: Helps organizations meet legal data protection standards.

ETHICS IN CYBERSECURITY



CYBERCRIME

Cybercrime is any criminal activity that involves a **computer or network**. It includes acts like **hacking, identity theft, online fraud, phishing, malware attacks, cyberbullying, and data breaches**, all intended to steal, damage, or manipulate data or systems.

Measures to Prevent Cybercrime >>

MACHINE INTELLIGENCE

Machine Intelligence refers to the ability of machines (especially computers and robots) to mimic or simulate human intelligence. It involves learning from data, making decisions, recognizing patterns, solving problems, and adapting to new inputs—mainly through techniques like machine learning, deep learning, and AI algorithms.

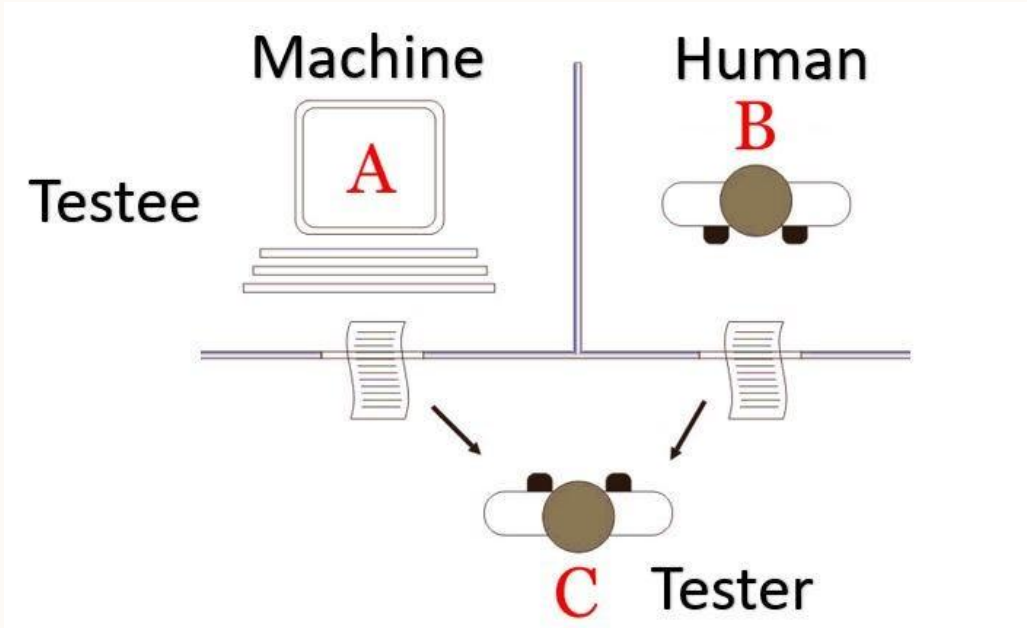
Aspect	Human Intelligence	Machine Intelligence
Nature	Biological, emotional, intuitive	Artificial, logical, data-driven
Learning	Based on experience, reasoning, emotions	Based on data and algorithms
Adaptability	Highly flexible and creative	Limited to what it is trained or programmed for
Decision-Making	Subjective, ethical, and emotion-influenced	Objective, based on algorithms and data
Error Handling	Can improvise and handle ambiguity	May fail without clear data or rules
Consciousness	Self-aware, conscious	Not conscious or self-aware

TURING TEST

The **Turing Test**, proposed by **Alan Turing** in 1950, is a method to assess a machine's ability to exhibit intelligent behavior equivalent to / indistinguishable from a human.

Method of the Turing Test:

- A human evaluator interacts with both a machine and a human through a computer interface (text-only, to avoid visual bias).
- If the evaluator cannot reliably tell which is which, the machine is said to have passed the Turing Test.
- The focus is on the machine's ability to mimic human conversation and behavior convincingly.



THANK YOU

Dr. Saptarshi Jana
Sr. Robotics Instructor
saptarshi.jana@techvein.com
mesaptarshi.jana@gmail.com