AI & NN
Unit II – Part 2

Topics : Knowledge representation using other logic – Structured representation of knowledge. Knowledge inference - Production based system, Frame based system.

Class: III CYS

Sem : 2025-26, Sem 5

-Dr. S.Durga, M.E., PhD

Recall…

- In **AI**, reasoning plays a crucial role in building systems that can **make decisions** and **infer knowledge** based on facts and conditions.
- **First-order logic (FOL)**, also known as predicate logic that **represent relationships between objects** and their **properties. It is** used for **knowledge representatio**n

Knowledge Representation

- Knowledge representation (KR) is a crucial aspect of artificial intelligence, as it involves encoding information about the world in a format that a computer system can utilize to solve complex tasks such as diagnosing a problem, understanding natural language, or playing a game.

Structured Representation of Knowledge:

Definition: Structured representations organize knowledge in a way that captures relationships, hierarchies, and dependencies among various entities or concepts.

Types of Structured Representations:

- **Semantic Networks**: Graph structures where nodes represent objects or concepts, and edges represent relationships among them (e.g., "is-a", "has-a").
  - **Example**: A semantic network might represent "A dog is a mammal" and "A mammal has fur."
- **Frames**: Data structures for representing stereotypical situations. A frame consists of various attributes or slots, which can have default values or be filled with specific values in particular situations.
  - **Example**: A frame for "Car" might have slots for "Make", "Model", "Color", and "Owner", allowing specific instances to be populated with actual data (e.g., Ford, Fiesta, Red, Alice).
- **Ontologies**: Formal representations of a set of concepts within a domain, and the relationships between those concepts, serving to share common vocabularies for knowledge representation.
  - **Example**: In a medical ontology, "Diabetes" could be related to "Symptoms", "Treatment", and "Causes".

Knowledge Inference

- Inference is the process of deriving new knowledge by applying logical rules to existing knowledge. This is critical in artificial intelligence for making decisions based on the represented knowledge.
- 2 types: **Production-Based System, frame-Based System:**

Production-Based System:

- A production system is an AI architecture that consists of a set of rules (productions) to derive conclusions from a set of known facts.
- **Components**:
  - **Rule**: A conditional statement typically expressed in the form “IF condition THEN action”.
    - **Example**: IF the light is on THEN the switch is up.
  - **Working Memory**: A set of facts that can be manipulated by the rules.
  - **Production Cycle**: The system's operation involves a cycle where it checks the working memory against the rules and applies applicable rules to derive new facts or actions.
- **Example of Use**: In a game-playing AI, a production system might check if a player's move was valid and then update the game board accordingly.

Frame-Based System:

- A frame-based system utilizes frames to represent stereotypical situations and allows inheritance of properties from more general to more specific instances.
- **Features**:
  - **Slots and Fillers**: Slots in frames can hold values or pointers to other frames, which allows for organizing information hierarchically.
  - **Defaults and Inheritance**: Frames can have default values that can be overridden by specific instances, and more specific frames can inherit attributes from more general frames.

  Example: A frame for "Animal" could have slots for "Species", "Habitat", and "Diet", and a frame for "Dog" (subordinate class) could inherit these slots while specifying specific values (e.g., "Species: Canine", "Habitat: Domestic", "Diet: Omnivore").

Recall

- Knowledge representation and inference are foundational to artificial intelligence, enabling systems to emulate human understanding and reasoning.
- Structured representations like semantic networks, frames, and ontologies provide ways to organize knowledge effectively
- systems based on production rules and frames support the process of inference, allowing AI to generate conclusions and make decisions based on their knowledge base.

Structured Representations of Knowledge in Cyber security

- **Attack Taxonomies**:
  - Example: The MITRE ATTACK framework categorizes different tactics, techniques, and procedures that adversaries use in real-world attacks. This structured representation helps security teams understand potential threats to their systems and respond appropriately.
- **Security Policies**:
  - Example: A structured representation of security policies using a markup language like XACML (eXtensible Access Control Markup Language) can define access control rules clearly. This allows organizations to enforce policies consistently across their IT environment.
- **Threat Models**:
  - Example: STRIDE model (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) is a structured way to identify and categorize security threats systematically. It helps analysts to think about threats more comprehensively, providing a structured approach to risk assessment.

Knowledge Inference in Cybersecurity

- **Intrusion Detection**:
  - Example: A system might infer that a user account is compromised based on a combination of unusual login patterns, unusual access to resources, and other contextual information.
  - For instance, if user “A” logs in from multiple geographical locations in a short period, the system could infer sophistication (e.g., potential credential theft) leading to triggering alerts.
- **Threat Intelligence Aggregation**:
  - Example: An organization may collect threat intelligence from multiple sources. Using inference rules, it can realize that recent malware activity in its region could indicate an elevated risk. This could lead to updating defenses, patching vulnerabilities, or conducting additional monitoring.

AI Models Used in Cyber security

- **Anomaly Detection Algorithms**:
  - Example: Anomaly detection models, such as Isolation Forest or One-Class SVM, can be used to identify deviations from normal behavior patterns in network traffic indicative of potential data breaches or insider threats.
- **Natural Language Processing (NLP)**:
  - Example: NLP models can analyze threat reports, security blogs, and forums to extract insights about emerging threats. For instance, using transformer-based models like BERT or GPT for sentiment analysis can help security analysts gauge the level of threat posed by new vulnerabilities mentioned online.
- **Generative Adversarial Networks (GANs)**:
  - Example: GANs can be used to simulate attack patterns to generate synthetic data for training intrusion detection systems, helping these systems become more robust against novel attacks.
- **Deep Learning Models**:
  - Example: Convolutional Neural Networks (CNNs) can classify traffic patterns and detect malware through static or dynamic analysis of executables. Companies might use these models to classify files as malicious or benign based on their features.
- **Graph-Based Neural Networks**:
  - Example: Graph Neural Networks (GNNs) can model relationships between users, devices, and transactions in a system. This is beneficial in identifying compromised accounts or unusual behavior patterns in a network, enhancing suspicious activity detection.