Reg.No | | | | | | | |

SNS COLLEGE OF TECHNOLOGY

(Autonomous)

Internal Assessment –III (May 2024)

Academic Year 2023-2024(Even) / SixthSemester

19CSE303 – ARTIFICIAL INTELLIGENCE

A

Time: $1^{1/2}$ Hours **Maximum Marks: 50**

Answer All Questions

No.	Question	CO	BL
1	**What are Bayesian networks, and how do they model uncertainty?** Bayesian networks are graphical models that use probability to represent relationships between variables and model uncertainty.	CO4	Und
2	**Provide an example of how a semantic network can represent relationships between concepts.** A semantic network can represent relationships between concepts like "dog" and "animal" with nodes for each concept connected by an "is-a" link.	CO4	Ana
3	**How do temporal models handle uncertainty over time?** Temporal models use probability distributions or intervals to represent uncertainty about when events will occur.	CO4	Ana
4	**Assess the role of human oversight in AI-based security systems.** Human oversight is critical for AI security systems to ensure accuracy, ethics, and address limitations of AI.	CO5	Ana
5	**Compare and contrast the effectiveness of various AI-based security measures.** AI-based security excels at adapting to new threats while automation improves efficiency, but interpretability and potential bias remain challenges**.**	CO5	Ana

PART - A (5 x 2 = 10 Marks)

PART - B (2 x 13 = 26, 1 X 14 = 14 Marks)

6 (a) Analyze the advantages and disadvantages of using semantic networks for knowledge representation. Provide a detailed comparison with other knowledge representation schemes such as rule-based systems. **Advantages of Semantic Networks:** — **CO4** **Ana**

- **Intuitive and Human-Friendly:** Concepts are depicted as nodes, and relationships between them are shown as labeled arcs. This visual representation makes it easy for humans to understand and modify the knowledge base.
- **Efficient Knowledge Organization:** Related concepts are grouped together, facilitating efficient retrieval and exploration of knowledge.
- **Scalability and Easy Extension:** New concepts and relationships can be readily incorporated into the network by adding new nodes and arcs.
- **Inheritance:** Properties of parent nodes can be automatically inherited by child nodes, reducing redundancy.

Disadvantages of Semantic Networks:

- **Limited Expressiveness:** While good for representing certain relationships, semantic networks struggle with complex logical reasoning tasks. Representing negation, disjunction ("or"), and quantifiers ("all," "some") can be cumbersome.
- **Limited Inference Capabilities:** Reasoning within the network can be computationally expensive, especially for large knowledge bases, as it often involves traversing the entire network.

- **Ambiguity in Link Labels:** The meaning of link labels might not be universally understood, leading to interpretation issues.
- **Scalability Issues with Large Domains:** As the network grows, managing it and ensuring consistency can become challenging.

Comparison with Rule-Based Systems:

- **Representation:** Semantic networks use a graphical structure, while rule-based systems rely on explicit if-then rules.
- **Inference:** Reasoning in semantic networks involves traversing the network, whereas rule-based systems employ a rule-matching process.
- **Expressiveness:** Rule-based systems offer more expressive power for complex logic due to their ability to handle negation, disjunction, and quantifiers more effectively.
- **Scalability:** Large rule-based systems can become cumbersome to maintain and debug.

Choosing the Right Approach:

The choice between semantic networks and rule-based systems depends on the specific application.

- **Semantic networks** are well-suited for tasks requiring:
    - Easy knowledge representation and visualization
    - Inheritance of properties
    - Efficient handling of specific relationships between concepts
- **Rule-based systems** excel in scenarios demanding:
    - Complex logical reasoning and inference
    - Precise control over knowledge representation

(Or)

(b) **Investigate the role of Bayesian networks in causal modeling and inference. Discuss how causal relationships are represented and inferred in Bayesian networks, and provide examples from fields such as epidemiology, economics, or social sciences.** **CO4** **Ana**

Bayesian networks (BNs) are powerful tools for representing and inferring causal relationships between variables. They offer a clear graphical framework and probabilistic foundation for understanding cause-and-effect.

Structure of a Bayesian Network:

- **Directed Acyclic Graph (DAG):** A BN consists of a DAG where:
    - **Nodes** represent random variables (e.g., disease, weather, economic factors).
    - **Edges** (arrows) represent causal relationships between variables. An arrow points from cause to effect.
- **Conditional Probability Tables (CPTs):** Each node has a CPT that specifies the probability of its state given the states of its parent nodes (variables with incoming arrows).

Causal Representation and Inference:

- **Encoding Causal Direction:** The direction of arrows encodes causal flow. A variable can only be influenced by its parents, not its descendants.

- **Inference:** BNs allow us to calculate the probability of any variable given evidence (observations on other variables) using Bayes' rule and the chain rule of probability. This enables us to estimate the effect of manipulating a cause variable on the outcome variable..

<table>
<tr><td>7</td><td>(a)</td><td>Evaluate the impact of Explainable AI techniques on the trustworthiness of Crime Prevention Camera systems, considering their ability to provide interpretable insights into decision-making processes.

Key Points:

• Explainable AI (XAI): Briefly define XAI and its role in making AI models more transparent and understandable.
• Trustworthiness of Crime Prevention Cameras: Discuss the current concerns regarding the trustworthiness of crime prevention cameras, such as:
    o Black Box Problem: Current AI models often operate as "black boxes," making it difficult to understand how they reach decisions. This lack of transparency can lead to mistrust.
    o Bias: AI models can inherit biases from the data they are trained on. This can lead to unfair profiling and discrimination.
• Impact of XAI: Explain how XAI techniques can address these concerns and improve trustworthiness:
    o Increased Transparency: XAI can provide insights into the factors influencing the camera's decisions, allowing for scrutiny and potential improvement.
    o Mitigating Bias: By understanding how the model arrives at its conclusions, bias can be identified and addressed during development or deployment.
    o Accountability: XAI fosters accountability by enabling human oversight and making it easier to identify potential errors or misuse.
• Limitations of XAI: Acknowledge that XAI is still an evolving field with limitations:
    o Complexity: Explaining complex AI models can be challenging for non-experts.
    o Trade-off: In some cases, achieving high accuracy might come at the expense of explainability.
• Conclusion: Despite limitations, XAI has the potential to significantly improve the trustworthiness of crime prevention camera systems. By fostering transparency, accountability, and fairness, XAI can build public trust and ensure the responsible use of these technologies</td><td>CO5</td><td>App</td></tr>
<tr><td></td><td></td><td>(Or)</td><td></td><td></td></tr>
<tr><td></td><td>(b)</td><td>Design a Decision Tree model for Crime Prevention Cameras, considering various factors such as location, time of day, and suspicious activities, and explain how it contributes to improving security outcomes.

Goal: To predict areas with a higher likelihood of criminal activity and optimize camera placement for improved security.

Features:

• Location: (e.g., Park, Alleyway, Bank, High-traffic intersection)
• Time of Day: (e.g., Weekday daytime, Weekend night, Early morning hours)
• Suspicious Activity: (e.g., Loitering, Groups gathering late at night, Forced entry attempts)
• Historical Crime Data: (e.g., Number of past incidents, Type of crimes)
• Lighting Conditions: (e.g., Well-lit, Poorly lit)</td><td>CO5</td><td>App</td></tr>
</table>

Decision Tree Structure:

1. **Root Node:** Represents all potential locations for camera placement.
2. **Splitting Rules:** Each node will split based on a specific feature, asking a yes/no question. (e.g., Is the location a park?)
3. **Terminal Nodes (Leaves):** These represent the final decision on camera placement (High Priority, Medium Priority, Low Priority).

Example Splitting Rules:

- **Is the location a high-crime area (based on historical data)?**
    - Yes: Is it a poorly lit alleyway?
        - Yes: High Priority for camera placement.
        - No: Medium Priority.
    - No: Is it a park with reported loitering after dark?
        - Yes: Medium Priority.
        - No: Low Priority.

How it Improves Security Outcomes:

- **Targeted Camera Placement:** Places cameras in areas with a higher predicted risk of crime, maximizing their effectiveness.
- **Focus on Suspicious Activity:** Alerts security personnel when suspicious activity is detected, allowing for quicker response times.
- **Data-Driven Decisions:** Provides objective data on crime trends to inform security strategies.

Benefits:

- **Reduced Crime Rates:** Deters criminal activity and increases the likelihood of apprehension.
- **Improved Resource Allocation:** Optimizes security resources like patrol frequency.
- **Enhanced Public Safety:** Creates a safer environment for the community.

Limitations:

- **Data Quality:** Relies on the accuracy of historical crime data and reported suspicious activities.
- **False Positives:** May trigger alerts for non-criminal activity.
- **Privacy Concerns:** Requires careful consideration of privacy regulations and balancing security needs with public privacy.

8 (a) **ABC Manufacturing operates a large facility with multiple machines critical for its production process. To ensure minimal downtime and optimal performance, ABC Manufacturing is exploring the implementation of a predictive maintenance system. As a data scientist consultant, you are tasked with designing a comprehensive solution leveraging probabilistic reasoning and machine learning techniques.Discuss how these metrics can be used to assess the system's accuracy, reliability, and cost-effectiveness in reducing downtime and maintenance costs.**

1. **Accuracy**:
    - **True Positives (TP)**: Instances where the predictive maintenance system correctly identifies an imminent machine failure, leading to proactive maintenance.
    - **True Negatives (TN)**: Instances where the system correctly identifies that no maintenance is required, and the machine continues to operate normally.
    - **False Positives (FP)**: Instances where the system predicts maintenance is needed, but no failure occurs, resulting in unnecessary downtime and maintenance costs.
    - **False Negatives (FN)**: Instances where the system fails to predict a machine failure, leading to unexpected downtime and potentially higher repair costs.
    - Accuracy can be assessed using metrics such as accuracy, precision, recall, and F1-score, which provide insights into the system's ability to correctly predict machine failures while minimizing false alarms.
2. **Reliability:**
    - Reliability refers to the consistency and stability of the predictive maintenance system over time.
    - Assess the system's performance over different time periods, environmental conditions, and machine types to ensure consistent results.
    - Use reliability metrics such as mean time between failures (MTBF) and mean time to repair (MTTR) to evaluate the system's ability to predict failures and minimize downtime.
3. **Cost-Effectiveness:**
    - Evaluate the cost savings achieved through the implementation of the predictive maintenance system compared to traditional reactive maintenance.
    - Consider factors such as reduced downtime, lower maintenance costs, extended machine lifespan, and improved production efficiency.
    - Conduct a cost-benefit analysis to quantify the financial impact of implementing the predictive maintenance system, taking into account initial setup costs, ongoing maintenance costs, and potential savings.
4. **Additional Metrics:**
    - Other metrics to consider include mean absolute error (MAE), root mean square error (RMSE), and area under the receiver operating characteristic curve (AUC-ROC) for assessing the predictive model's performance.
    - Monitor key performance indicators (KPIs) such as equipment utilization, production output, and overall equipment effectiveness (OEE) to gauge the system's impact on production efficiency.

(b) **A residential neighborhood is experiencing a series of break-ins, prompting homeowners to invest in AI-based Home Security systems. How can Neural Net Learning algorithms continuously analyze sensor data from smart doorbell cameras and motion detectors to distinguish between normal activities and potential security breaches? Evaluate the reliability and scalability of Neural Net Learning in real-time home security applications.**

Data Preprocessing:

- Before feeding data into neural networks, preprocess the sensor data to remove noise, normalize values, and extract relevant features. This can involve techniques like background subtraction, image resizing, and feature extraction.

Neural Network Architecture:

- Design neural network architectures suitable for processing sensor data. For image data from smart doorbell cameras, convolutional neural networks (CNNs) are commonly used. For motion sensor data, recurrent neural networks (RNNs) or Long Short-Term Memory (LSTM) networks may be applicable.
- Utilize multiple layers with appropriate activation functions to capture complex patterns and relationships in the data.

Training and Learning:

- Train the neural network using labeled data, where normal activities are labeled as negative examples and security breaches are labeled as positive examples.
- Employ techniques such as backpropagation and gradient descent to update the network weights and minimize the loss function.
- Regularly update the model with new data to adapt to changing patterns and environments.

Real-Time Monitoring:

- Implement the trained neural network in a real-time monitoring system to continuously analyze incoming sensor data.
- Set appropriate thresholds for triggering alerts based on the neural network's output probabilities. For example, if the probability of a security breach exceeds a certain threshold, an alert is generated.

Reliability:

- Evaluate the reliability of neural net learning algorithms by measuring their accuracy, precision, recall, and false alarm rates over time.
- Conduct rigorous testing and validation to ensure the model can generalize well to unseen data and various environmental conditions.
- Implement redundancy and fail-safe mechanisms to handle unexpected failures or adversarial attacks.

Scalability:

- Neural net learning algorithms can be scaled horizontally by distributing the computational workload across multiple devices or nodes.
- Utilize cloud-based solutions or edge computing platforms to