DSAR Assignment 3

1. What types of AI-based business intelligence applications are currently used in

insurance?

* Predictive Underwriting: AI is used to assess risk factors, predict claims, and determine insurance premiums based on individual customer data.
* Fraud Detection: AI systems can detect fraudulent claims by analyzing patterns, anomalies, and historical data.
* Customer Service Chatbots: AI-powered chatbots assist customers with inquiries, policy information, and claim processing.
* Image Analysis: AI is used for claims processing by analyzing images and documents to expedite assessments.
* Personalized Policies: AI helps create personalized insurance policies tailored to a customer's specific needs.
* Risk Assessment: AI evaluates and assesses risks for better decision-making.

2. What are the applications and techniques of artificial intelligence?

* Applications: AI is used in various fields, including healthcare (diagnosis and treatment), finance (algorithmic trading), natural language processing (chatbots), autonomous vehicles, recommendation systems, and more.
* Techniques: AI techniques include machine learning (supervised, unsupervised, reinforcement learning), deep learning, natural language processing, computer vision, and more.

3. What is the difference between security and surveillance?

* Security refers to measures taken to protect against threats, risks, or vulnerabilities, which can include physical security, cybersecurity, and data protection.
* Surveillance is the act of monitoring, observing, or recording activities, behaviors, or events. It is a component of security and is used to detect and prevent security breaches.

4. Can AI be used for security?

Yes, AI can be used for security in various domains, including cybersecurity, physical security, and data security. AI systems can analyze data, detect anomalies, and respond to security threats in real-time.

5. How does AI improve security?

* Threat Detection: AI can identify and respond to security threats faster and more accurately than traditional methods by analyzing vast amounts of data for anomalies.
* Anomaly Detection: AI can detect unusual patterns or behaviors that may indicate a security breach, even in large datasets.
* Automation: AI can automate security processes, such as incident response, reducing human intervention and response time.
* Predictive Analysis: AI can predict and prevent security threats based on historical data and patterns.
* Enhanced Authentication: AI enables advanced authentication methods like facial recognition and biometrics for secure access.
* Real-time Monitoring: AI systems continuously monitor for security events, providing immediate responses when necessary.

Top of Form

Bottom of Form