GLOBAL INDUSTRIES INTELLIGENCE

APPLICATIONS OF AI FOR ANOMALY DETECTION

+44 2080 508 945 www.giintelligence.com training@giintelligence.com

COURSE OUTLINES

This course provides an in-depth understanding of anomaly detection using Artificial Intelligence (AI) and its various applications in real-world scenarios. Participants will learn how AI can be leveraged to identify anomalies in large datasets, detect fraudulent activities, and improve operational efficiency across different industries such as finance, healthcare, manufacturing, and cybersecurity

DAY 2: INTRODUCTION TO ANOMALY DETECTION AND AI

- **Overview of Anomaly Detection**
  - Definition of anomaly detection: What is an anomaly and why is it important?
  - Types of anomalies: Point anomalies, contextual anomalies, and collective anomalies
  - Applications of anomaly detection: Fraud detection, network security, predictive maintenance, and more

- **AI and Machine Learning Fundamentals for Anomaly Detection**
  - Key AI techniques used in anomaly detection: Supervised vs. unsupervised learning
  - Introduction to machine learning models: Decision trees, k-nearest neighbors (KNN), clustering methods
  - Overview of deep learning techniques: Autoencoders, neural networks, and recurrent neural networks (RNNs)
  - Data preprocessing for anomaly detection: Feature engineering, normalization, and scaling

- **Challenges in Anomaly Detection**
  - The imbalance problem: Handling rare anomalies in large datasets
  - High-dimensional data and curse of dimensionality
  - Noise and outliers in the data: Strategies to manage data quality issues

DAY 2: TECHNIQUES FOR ANOMAL DETECTION USING AI

- **Supervised Learning for Anomaly Detection**
  - Supervised anomaly detection: Labeling and classification techniques
  - Key algorithms: Decision Trees, Random Forest, Support Vector Machines (SVM), and Logistic Regression
  - Performance evaluation: Precision, recall, F1-score, and confusion matrix
  - Handling class imbalance using sampling techniques (e.g., SMOTE, undersampling)

- **Unsupervised Learning for Anomaly Detection**
  - Overview of unsupervised anomaly detection techniques
  - Clustering algorithms: K-means, DBSCAN, and hierarchical clustering
  - Density-based methods: One-Class SVM, Isolation Forest
  - Distance-based methods: K-Nearest Neighbors (KNN)

- **Deep Learning for Anomaly Detection**
  - Autoencoders for anomaly detection: Architecture, training, and applications
  - Recurrent Neural Networks (RNNs) for time series anomaly detection
  - Long Short-Term Memory (LSTM) networks for sequence anomalies
  - Practical application: Anomaly detection using deep learning models

DAY 3: REAL-WORLD APPLICATIONS OF AI FOR ANOMALY DETECTION

- **Fraud Detection in Finance and Banking**
  - Overview of financial fraud: Credit card fraud, transaction fraud, money laundering
  - Using AI for detecting fraudulent transactions: Supervised and unsupervised approaches
  - Application of anomaly detection in monitoring suspicious behavior
  - Case study: Building a fraud detection system using machine learning

- **Anomaly Detection in Cybersecurity**
  - Detecting network intrusions and cyberattacks using anomaly detection
  - Identifying unusual access patterns, data exfiltration, and malware activity
  - Applications of AI in intrusion detection systems (IDS)
  - Case study: Anomaly-based intrusion detection in a corporate network

- **Healthcare and Medical Anomaly Detection**
  - Identifying medical anomalies: Detecting outliers in patient data, diagnostics, and monitoring
  - AI in detecting unusual patterns in patient vitals, medical images, and test results
  - Predictive analytics for detecting rare diseases and health anomalies
  - Case study: AI-driven anomaly detection for early disease diagnosis

DAY 4: IMPLEMENTING AND DEPLOYING AI MODELS FOR ANOMALY DETECTION

- **Building an AI Anomaly Detection System**
  - Step-by-step guide to building an anomaly detection system: Data collection, model selection, and training
  - Model evaluation and tuning: Hyperparameter optimization, cross-validation
  - Handling model drift and continuous learning in anomaly detection
  - Deploying AI models for real-time anomaly detection in production environments

- **Tools and Frameworks for Anomaly Detection**
  - Overview of popular AI libraries and tools for anomaly detection: TensorFlow, Keras, Scikit-learn, PyTorch
  - Pre-built models and frameworks for anomaly detection: Isolation Forest, One-Class SVM, DBSCAN
  - Integrating anomaly detection models with enterprise systems for automated monitoring

- **Interpretability and Explainability of AI Models**
  - Importance of interpretability in anomaly detection models
  - Techniques for explaining AI model decisions: SHAP values, LIME, partial
  - dependence plots
  - Case studies of interpretable anomaly detection models in healthcare and finance

DAY 5: ADVANCED TOPICS AND FUTURE TRENDS IN ANOMALY DETECTION

- **Anomaly Detection in Big Data**
  - Handling large-scale data and distributed anomaly detection systems
  - Techniques for anomaly detection in streaming data (e.g., Kafka, Spark)
  - Real-time anomaly detection in Internet of Things (IoT) and sensor networks

- **Anomaly Detection for Predictive Maintenance**
  - Using AI for predictive maintenance in industrial IoT applications
  - Monitoring machinery and equipment for early failure detection
  - Case study: AI-powered anomaly detection for equipment failure prediction in manufacturing

- **Future Trends and Challenges**
  - Emerging trends in AI and anomaly detection: Federated learning, explainable AI, reinforcement learning
  - The evolving role of AI in cybersecurity and threat intelligence
  - Ethical considerations and challenges in the use of AI for anomaly detection

ADDITIONAL COURSE DETAILS:

- **Target Audience:**
  - Data scientists, machine learning engineers, and AI practitioners interested in anomaly detection
  - Business analysts and operational managers working with large datasets
  - Professionals in sectors such as finance, cybersecurity, healthcare, and manufacturing, looking to leverage AI for anomaly detection
  - IT professionals and decision-makers focused on adopting AI solutions for fraud detection, predictive maintenance, and monitoring