



PB INSTITUTE OF RESEARCH AND TECHNOLOGY

P.O Box 21457-00100

Nairobi - Kenya

Mobile: +254 721 214 795

Email: info@pebblesinstitute.org

Advanced Fraud Analytics & Anomaly Detection

Duration: 10 days

On-Site

01 Who Should Attend

- Data analysts
- Risk analysts
- Financial crime professionals
- Internal auditors
- Compliance professionals
- Cybersecurity professionals
- Data engineers
- Business intelligence professionals
- Banking and financial services professionals
- Insurance professionals
- Risk and governance managers
- Technology and analytics managers



PB INSTITUTE OF RESEARCH AND TECHNOLOGY

P.O Box 21457-00100

Nairobi - Kenya

Mobile: +254 721 214 795

Email: info@pebblesinstitute.org

02 About the Course

This advanced training equips professionals with the knowledge and practical skills to **design, implement, and manage enterprise fraud analytics and anomaly detection systems**. The course combines data analytics, statistical modelling, machine learning, behavioral analysis, and real-time monitoring to help organizations identify suspicious activities and emerging fraud patterns. Participants will explore fraud data preparation, anomaly detection techniques, supervised and unsupervised machine learning, behavioral profiling, risk scoring, real-time analytics, alert management, model evaluation, and system deployment. The training emphasizes scalable, explainable, and adaptive fraud detection frameworks suitable for financial services, insurance, e-commerce, telecommunications, government, and other high-risk environments.

03 Workshop Objectives

- Understand the fundamentals of anomaly detection and fraud analysis.
- Master statistical methods for outlier detection.
- Utilize machine learning algorithms for anomaly detection.
- Implement real-time anomaly detection systems.
- Design and build fraud analysis models for various applications.
- Optimize detection models for accuracy and efficiency.
- Troubleshoot and address complex anomaly detection challenges.
- Implement model evaluation and validation techniques for fraud analysis.
- Integrate anomaly detection into real-world systems.
- Understand how to handle imbalanced datasets in fraud detection.
- Explore advanced anomaly detection techniques (e.g., autoencoders, isolation forests).
- Apply real world use cases for anomaly detection and fraud analysis.



PB INSTITUTE OF RESEARCH AND TECHNOLOGY

P.O Box 21457-00100

Nairobi - Kenya

Mobile: +254 721 214 795

Email: info@pebblesinstitute.org

04 Module Topics

Module 1: Introduction to Anomaly Detection and Fraud Analysis

- Fundamentals of anomaly detection and fraud analysis.
- Overview of statistical and machine learning methods.
- Setting up an anomaly detection development environment.
- Introduction to detection libraries and tools.
- Best practices for anomaly detection.

Module 2: Statistical Methods for Outlier Detection

- Implementing statistical methods for outlier detection (Z-score, IQR).
- Utilizing distribution-based methods for anomaly detection.
- Designing and building statistical anomaly detection pipelines.
- Optimizing statistical methods for data analysis.
- Best practices for statistical methods.

Module 3: Machine Learning Algorithms for Anomaly Detection

- Implementing machine learning algorithms for anomaly detection (One-Class SVM, DBSCAN).
- Utilizing unsupervised learning for anomaly detection.
- Designing and building machine learning detection models.
- Optimizing machine learning models for fraud detection.
- Best practices for machine learning.

Module 4: Real-Time Anomaly Detection Systems

- Implementing real-time anomaly detection systems.
- Utilizing streaming data processing for real-time analysis.
- Designing and building real-time detection pipelines.
- Optimizing real-time systems for low latency detection.
- Best practices for real-time detection.



PB INSTITUTE OF RESEARCH AND TECHNOLOGY

P.O Box 21457-00100

Nairobi - Kenya

Mobile: +254 721 214 795

Email: info@pebblesinstitute.org

Module 5: Fraud Analysis Model Design

- Designing fraud analysis models for specific applications.
- Implementing model architectures for various fraud scenarios.
- Utilizing feature engineering for fraud detection.
- Optimizing model design for fraud prevention.
- Best practices for model design.

Module 6: Model Optimization for Accuracy and Efficiency

- Optimizing detection models for accuracy and efficiency.
- Utilizing hyperparameter tuning for detection models.
- Implementing model compression and acceleration.
- Designing scalable detection solutions.
- Best practices for model optimization.

Module 7: Troubleshooting Anomaly Detection Challenges

- Debugging complex anomaly detection issues.
- Analyzing model performance and errors.
- Utilizing troubleshooting techniques for model improvement.
- Resolving common anomaly detection challenges.
- Best practices for troubleshooting.

Module 8: Model Evaluation and Validation for Fraud Analysis

- Implementing evaluation metrics for fraud analysis tasks.
- Utilizing cross-validation techniques for detection models.
- Designing and building model validation pipelines.
- Optimizing model evaluation strategies.
- Best practices for model evaluation.

Module 9: Integration with Real-World Systems



PB INSTITUTE OF RESEARCH AND TECHNOLOGY

P.O Box 21457-00100

Nairobi - Kenya

Mobile: +254 721 214 795

Email: info@pebblesinstitute.org

- ▶ Integrating anomaly detection models into real-world applications.
- ▶ Utilizing APIs and deployment tools for detection systems.
- ▶ Implementing real-time fraud detection systems.
- ▶ Optimizing models for deployment environments.
- ▶ Best practices for integration.

Module 10: Handling Imbalanced Datasets in Fraud Detection

- ▶ Implementing techniques for handling imbalanced datasets.
- ▶ Utilizing oversampling and undersampling methods.
- ▶ Designing and building robust models for imbalanced data.
- ▶ Optimizing data handling for fraud detection.
- ▶ Best practices for imbalanced data.

Module 11: Advanced Anomaly Detection Techniques

- ▶ Implementing autoencoders for anomaly detection.
- ▶ Utilizing isolation forests for outlier detection.
- ▶ Designing and building advanced detection models.
- ▶ Optimizing advanced techniques for specific tasks.
- ▶ Best practices for advanced techniques.

Module 12: Real-World Use Cases

- ▶ Implementing anomaly detection for financial fraud.
- ▶ Utilizing anomaly detection for network intrusion detection.
- ▶ Implementing anomaly detection for healthcare fraud.
- ▶ Utilizing anomaly detection for manufacturing quality control.
- ▶ Best practices for real-world applications.

Module 13: Detection Libraries Implementation



PB INSTITUTE OF RESEARCH AND TECHNOLOGY

P.O Box 21457-00100

Nairobi - Kenya

Mobile: +254 721 214 795

Email: info@pebblesinstitute.org

- ▶ Utilizing scikit-learn for anomaly detection tasks.
- ▶ Implementing detection models with TensorFlow and PyTorch.
- ▶ Designing and building detection pipelines with libraries.
- ▶ Optimizing library usage for efficient implementation.
- ▶ Best practices for library implementation.

Module 14: Model Interpretability for Anomaly Detection

- ▶ Implementing model interpretability techniques for detection models.
- ▶ Utilizing visualization tools for understanding detected anomalies.
- ▶ Designing and building interpretable detection models.
- ▶ Optimizing model transparency.
- ▶ Best practices for model interpretability.

Module 15: Future Trends in Anomaly Detection and Fraud Analysis

- ▶ Emerging trends in anomaly detection and fraud analysis.
- ▶ Utilizing graph-based anomaly detection.
- ▶ Implementing federated learning for distributed fraud detection.
- ▶ Best practices for future applications.