Professional Certificate in AI in Financial Crime Compliance

Deep Learning Applications in Financial Crime Prevention

Anomaly Detection: The process of identifying unusual patterns that do not conform to expected behavior, called outliers. It has many applications in financial crime prevention, including the detection of unusual transactions, account behavior, and money laundering activities.

Artificial Neural Networks (ANNs): A computing system inspired by the human brain's biological neural networks. ANNs consist of input and output layers, as well as (in most cases) a hidden layer consisting of units that transform the input into something the output layer can use. They are used in deep learning for financial crime prevention to model complex relationships between variables and make predictions or decisions without being explicitly programmed to perform the task.

Autoencoder: A type of artificial neural network used for learning efficient codings of input data. It's typically used for dimensionality reduction or denoising. In financial crime prevention, autoencoders can be used to detect anomalies by training them on normal transaction data and then using them to reconstruct new transactions. The difference between the input and the output can be used as a measure of anomalous behavior.

Boltzmann Machines: A type of stochastic recurrent neural network and a restricted form of Hopfield network. A Boltzmann machine is a generative model that can learn internal representations of data, and it is often used for dimensionality reduction, classification, regression, collaborative filtering, feature learning, and topic modeling. In financial crime prevention, Boltzmann machines can be used to detect anomalies or to learn patterns in data that can be used for prediction or decision making.

Convolutional Neural Networks (CNNs): A class of deep, feed-forward artificial neural networks that have shown to be effective in areas such as image recognition and classification. CNNs have a special architecture that includes one or more convolutional layers, often followed by pooling (downsampling) layers, fully connected layers, and normalization layers. In financial crime prevention, CNNs can be used to detect patterns in data, such as images of checks or identity documents, or to classify transactions as fraudulent or non-fraudulent.

Deep Learning: A subset of machine learning that is based on artificial neural networks with representation learning. It can process a wide range of data resources, requires less data preprocessing by humans, and can often produce more accurate results than traditional machine learning approaches. Deep learning is used in financial crime prevention for tasks such as anomaly detection, fraud detection, and anti-money laundering.

Deep Neural Networks (DNNs): A type of artificial neural network with many layers (i.e., depth) that are trained using a large set of data. DNNs are capable of learning complex patterns and representations from

data and are used in a variety of applications, including financial crime prevention.

Generative Adversarial Networks (GANs): A class of artificial neural networks used in unsupervised machine learning, implemented by a system of two neural networks contesting with each other in a zero-sum game framework. GANs can learn to mimic any distribution of data and have many applications in financial crime prevention, including the generation of synthetic data for training other models, the detection of anomalies, and the generation of new transactions that are similar to those in a training set.

Long Short-Term Memory (LSTM): A type of recurrent neural network (RNN) that is capable of learning long-term dependencies, which makes it useful for tasks such as speech recognition, machine translation, and natural language processing. LSTMs have a special architecture that includes memory cells and gates that can selectively forget or retain information over time. In financial crime prevention, LSTMs can be used to detect anomalies or to predict future behavior based on historical data.

Natural Language Processing (NLP): A field of artificial intelligence that focuses on the interaction between computers and humans through natural language. The ultimate objective of NLP is to read, decipher, understand, and make sense of human language in a valuable way. In financial crime prevention, NLP can be used to extract information from text data, such as reports of suspicious activity, and to classify or cluster transactions based on their text descriptions.

Recurrent Neural Networks (RNNs): A class of artificial neural networks that are capable of processing sequential data, such as time series or natural language. RNNs have a special architecture that includes feedback connections that allow them to maintain an internal state or memory over time. This makes them well-suited for tasks such as speech recognition, machine translation, and natural language processing. In financial crime prevention, RNNs can be used to detect anomalies or to predict future behavior based on historical data.

Restricted Boltzmann Machines (RBMs): A type of stochastic artificial neural network that can learn probability distributions over its inputs. It is a generative model that is often used for dimensionality reduction, collaborative filtering, feature learning, and topic modeling. RBMs consist of a visible layer and a hidden layer, and the connections between the layers are undirected. In financial crime prevention, RBMs can be used to detect anomalies or to learn patterns in data that can be used for prediction or decision making.

Supervised Learning: A type of machine learning that involves training a model on a labeled dataset, where the correct output or label is provided for each input. The goal of supervised learning is to learn a mapping from inputs to outputs that can be used to make predictions on new, unseen data. In financial crime prevention, supervised learning is used for tasks such as fraud detection, where a model is trained on a dataset of fraudulent and non-fraudulent transactions.

Transfer Learning: A machine learning technique where a pre-trained model is used as the starting point for a new model, instead of training a new model from scratch. Transfer learning is useful when there is limited data available for a task, or when a pre-trained model has already learned features that are useful for the new task. In financial crime prevention, transfer learning can be used to improve the performance of models

for tasks such as anomaly detection or fraud detection.

Unsupervised Learning: A type of machine learning that involves training a model on an unlabeled dataset, where the correct output or label is not provided for each input. The goal of unsupervised learning is to learn patterns or structures in the data that can be used for tasks such as clustering, dimensionality reduction, or anomaly detection. In financial crime prevention, unsupervised learning is used for tasks such as detecting unusual patterns or outliers in transaction data.

Word Embeddings: A type of word representation that allows words with similar meanings to have a similar representation. Word embeddings are learned from data and can be used in natural language processing tasks such as sentiment analysis, text classification, and machine translation. In financial crime prevention, word embeddings can be used to extract information from text data, such as reports of suspicious activity, and to classify or cluster transactions based on their text descriptions.