**How is Fraud Detected in the Banking System?**

There are various fraud detection methods that banks use, but some of the most common include suspicious activity reports, transaction monitoring, and data analytics.

**Suspicious Activity Reports (SARs)** are one of the primary ways that banks detect fraud. If a bank employee suspects that fraud is taking place, they will file a SAR. The SAR will then be reviewed by the bank's fraud department. If the fraud department determines that there is enough evidence to suggest that fraud has taken place, they will take appropriate action.

**Data analytics** is also increasingly being used by banks to detect fraud. By analyzing large data sets, banks can look for patterns that might indicate fraud. For example, if a customer suddenly starts making a lot of small transactions that are all just below their daily limit, this could be a sign that they are trying to avoid triggering fraud detection measures.

**Transaction monitoring** is another fraud detection measure that is commonly used by banks. Under transaction monitoring, banks will flag any transactions that seem unusual or out of the ordinary. For example, if a customer who usually only spends $50 per day suddenly starts spending $5,000 per day, this would be considered an unusual transaction. The transaction would then be flagged and reviewed by the fraud department to determine if fraud has taken place.

‍In the past decade, one of the most popular methods of fraud detection is to use machine learning algorithms. These algorithms are able to detect patterns of fraudulent behavior and flag questionable transactions. The SVM is the most widely financial fraud detection technique used in data mining, followed by both of Naïve Bayes and Random Forest. This indicates that the support vector machine technique is the leading DM technique utilized in fraud detection of the financial domains. (However, SVMs are supervised max-margin models that cannot be used on this dataset.) Jeragh and AlSulaimi(Jeragh & AlSulaimi, 2018) suggested a novel [unsupervised learning](https://www.sciencedirect.com/topics/computer-science/unsupervised-learning) model for identifying fraud in credit cards by combining OSVM with an autoencoder. The authors implemented the combined model on the Kaggle credit card dataset. (It contains only numerical input variables which are the result of a PCA transformation. Features V1, V2, … V28 are the principal components obtained with PCA, the only features which have not been transformed with PCA are 'Time' and 'Amount'. Feature 'Class' is the response variable and it takes value 1 in case of fraud and 0 otherwise.)

Supervised learning approaches were found to be better performance approaches than unsupervised approaches. This is mainly due to the limitation of studies that adopt financial fraud detection techniques utilizing outlier fraud detection because of the difficulty of detecting outliers.

**How do Lloyds Banking Group detect fraud?**

Lloyds Bank has rolled out a fraud prevention system, dubbed 'the Rat', that uses behavioural analysis to spot crooks and freeze them out of victims' accounts before they can make off with any money.

The Rat employs behavioural analysis to build a detailed profile of how a customer uses internet banking - for example how they usually move around the screen, or the time it takes them to enter their personal details.

This biometric data is combined in real-time with software which can detect if remote access is being used to access the customer’s computer. Finally, Lloyds says that it looks for a "secret sign" - an unnamed thing that fraudsters do that gives them away.

(I haven't found any information on what specific machine learning algorithms they used.)

Jeragh, M., & AlSulaimi, M. (2018). Combining Auto Encoders and One Class Support Vectors Machine for Fraudulant Credit Card Transactions Detection. 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), 178–184. https://doi.org/10.1109/WorldS4.2018.8611624