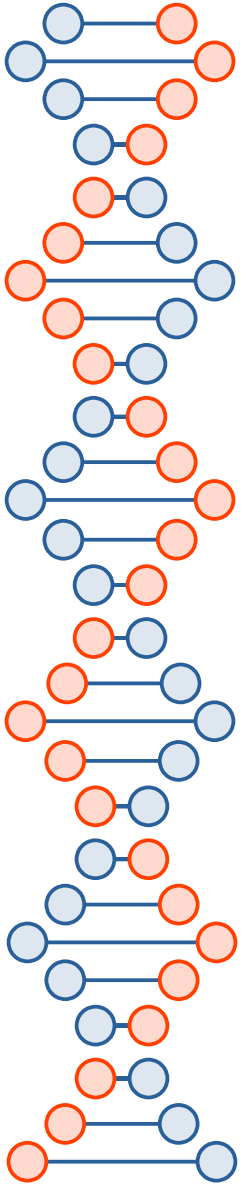
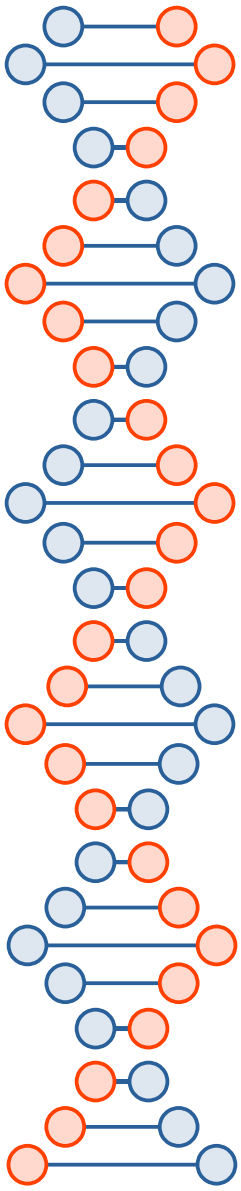
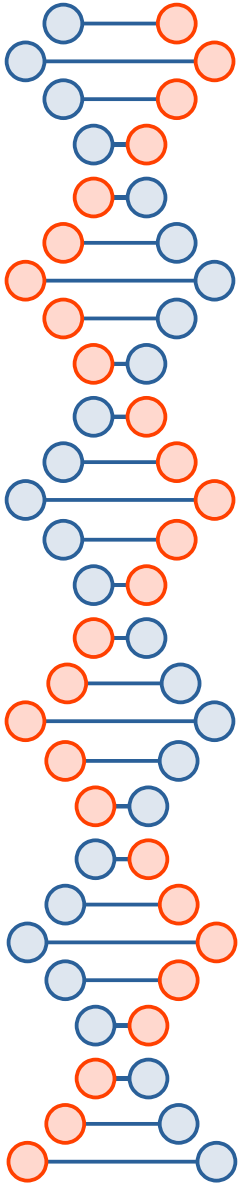


Fraud Detection in Banking



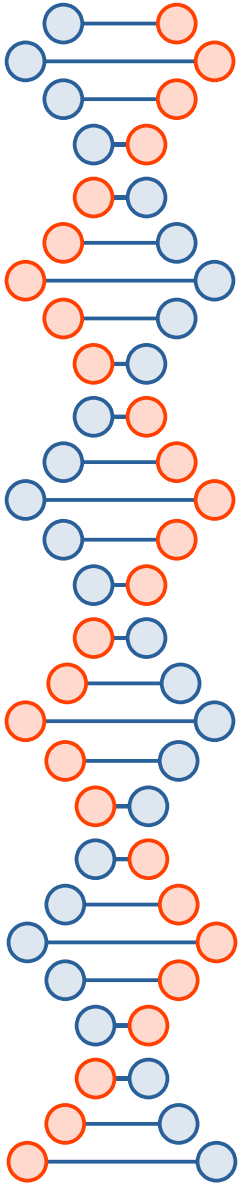
Data

- To detect fraudulent transactions in banking, we require diverse and high-quality data.



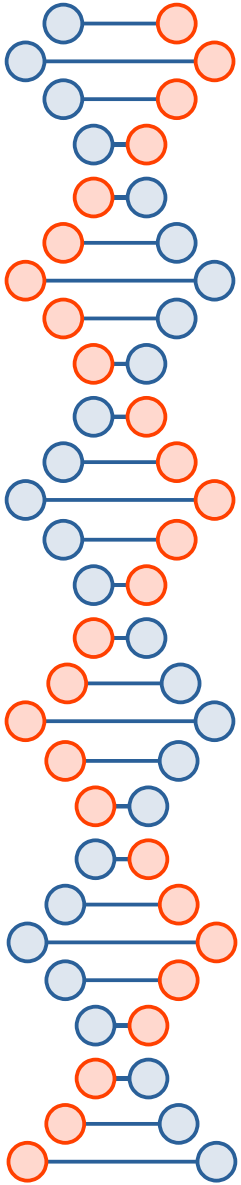
Data Sources :

- Transaction Logs: Records of all transactions, including timestamps, amounts, and locations.
- Customer Information: Demographic details, account history, and behavioral patterns.
- External Sources: Blacklists, credit scores, and regulatory databases.
- Device & Network Data: IP addresses, geolocation, and device fingerprints.



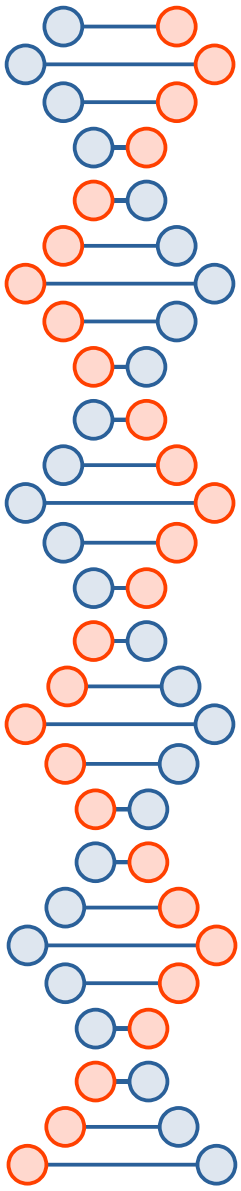
Data Issues :

- Missing Data: Some transactions may lack location or device details.
- Imbalanced Data: Fraudulent transactions are rare, making it difficult to train models effectively.
- Data Inconsistencies: Different formats in transaction logs from various banking systems.
- Privacy & Security Concerns: Customer data must be protected and comply with regulations (e.g., GDPR, PCI DSS).



Types of Data :

- Structured Data: Transaction records, customer profiles, account balances.
- Semi-structured Data: JSON logs from banking apps, email alerts for suspicious transactions.
- Unstructured Data: Customer complaints, call center logs, emails reporting fraud.



Problem Statement

- Fraudulent transactions cause significant financial losses for banks and customers. The challenge is to build an intelligent fraud detection system that can:
- Accurately identify fraudulent transactions while minimizing false positives.
- Process real-time data to detect anomalies instantly.
- Adapt to evolving fraud patterns using machine learning.
- Ensure compliance with financial regulations.