The data from several POS systems will be introduced into the architecture through a queuing system.

The queued data will be then consumed by the streaming data processing framework to authenticate the transaction and mark it as "Fraud" or "Genuine"

The Rules to be programmed into the streaming framework to identify the authenticity of transactions are as follows:

1. Upper Control Limit (UCL) :

Based on the previous transaction patterns of the card user, the maximum limit on the amount per transaction is used as a parameter to authenticate the transaction.

UCL = (Moving average) + 3 * (Standard deviation) {These are calculated for the last 10 transactions marked as genuine}

2. Credit Score:

The score field in the member_score table is used as a parameter to authenticate the transaction.

If score < 200, member is a defaulter and the transaction is rejected.

3. Zip Code distance:

The distance with respect to time between the current and previous transaction locations is used as a parameter to determine the authenticity of the transaction.

If the distance between the transaction locations with respect to time is greater than a particular threshold, then the transaction is marked as fraud.