

SEMINAR TEILCHENPHYSIK

Thema

Open-source Framework for Synthetic Fraud Datasets via Generative AI

Abstract

This work presents a flexible and open-source framework for simulating realistic banking transaction data, designed to address the dual challenges of data scarcity and privacy compliance in financial fraud research. Developed during an industry secondment at IBM France Lab Saclay, within the European SMARTHEP Network, our solution leverages Generative AI Agents to mimic both legitimate and fraudulent behaviors in temporal transaction sequences.

Initially based on Markov models, the framework has evolved into a Large Language Model (LLM)-driven architecture. A dedicated Strategist LLM defines behavioral blueprints for diverse profiles—such as everyday spenders, travelers, identity thieves, or money launderers. Then, an Agent LLM generates detailed, structured activities including transaction type, timestamp, location, amount, and contextual signals such as device or network anomalies. This two-stage design allows for flexible scenario generation and improved interpretability. To address limitations in output validity and formatting, we explored the use of lightweight LLMs for output validation and correction. This self-correcting mechanism aims to reduce invalid generations and enhance consistency.

The resulting synthetic datasets could offer a safe and configurable environment for developing and testing fraud detection strategies—without the constraints of proprietary banking data. In addition, exploratory thinking on applying automation principles and LLMs to LHC research and infrastructure will be presented, along with an overview of current community efforts.

Vortragender

Micol Olocco
TU Dortmund

Ort

CP-03-123

Zeit

Mittwoch, 16.07.2025
14:00 – 15:00 Uhr

im Auftrag:

Dr. Maik Becker