GSMA

Real-time On-device Vishing Detection and Anti-DeepVoice Protection

Case Study: LG Uplus

Case Study: LG Uplus

Real-time On-device Vishing Detection and Anti-DeepVoice Protection

Voice phishing has become an increasingly serious public harm issue, affecting ordinary consumers across a wide range of scenarios, including impersonation of financial institutions, government agencies, delivery services, family members, and other trusted parties.

At the same time, the rapid spread of deepfake and voice-cloning technologies has begun to reshape the fraud landscape. Major cases of deepfake and voice cloning have occurred in the financial industry.

This case study describes an on-device artificial intelligence solution developed to detect vishing and synthetic voice impersonation in real time during active phone calls.

The problem addressed is that vishing attacks have become increasingly sophisticated and context-dependent, while conventional fraud prevention methods have mainly relied on pre-call or post-call analysis of call metadata, traffic patterns, or user reports. As a result, many fraud attempts are not interrupted at the moment of attack, when users are most vulnerable.

Solution

To address this problem, real-world vishing crime data was acquired from relevant law enforcement agencies, including the Korean National Police Agency and the National Forensic Service. Before model training, all personally identifiable information was removed through a dedicated anonymisation engine, and the data was then used to train a lightweight on-device language model for binary classification, enabling the model to determine whether an ongoing conversation is likely to constitute vishing fraud.

In response, a hybrid multi-layered detection architecture was implemented. A number of artificial intelligence models were deployed to support both real-time vishing detection and anti-deepvoice protection, including on-device Voice Activity Detection (VAD), Speech-to-Text (STT), vishing detection, and Anti-DeepVoice modules. This enables the system to provide immediate warnings through sound alerts and pop-up notifications without transmitting voice data to a server.

The organisation developed and implemented a real-time fraud detection solution within its proprietary dialler application, ixi-O. The implementation team trained a compact language model on de-identified vishing crime data. The organisation also incorporated synthetic voice detection capabilities to identify impersonation attempts involving family members, friends, or public figures. The solution was fully implemented on-device, ensuring that audio data remained on the user's device at all times.

Impact:

The solution achieved a reported detection accuracy of 95 per cent while operating with a highly lightweight, quantized model architecture. This allowed real-time execution on mobile devices without materially affecting the user experience. LG Uplus also reported approximately 5,500 detection instances per month. The solution improved customer protection by providing warnings during live calls, increasing awareness at the point of attack, and strengthening trust in the mobile operator's ability to deliver proactive security.

Additional information	
Cost:	Low
MNO/Org:	LG U+
Location:	Asia Pacific
Tags:	Scam Call Detection and Blocking