GSMA

October 2025

Airtel use case: Fraud Detection Solution

Airtel use case: Fraud Detection Solution

The menace of spam and fraud is escalating at an alarming rate worldwide, with over 300 billion spam calls, a 250% surge in AI-driven voice scams, and $1.4 trillion in global banking fraud losses reported. India is no exception to this trend. The country has seen a dramatic rise in cyber threats, particularly spam and financial fraud propagated through malicious links. In just the first nine months of 2024, over 1.7 million cybercrime complaints were registered, with financial losses exceeding $1.2 billion (I4C). Projections for 2025 estimate 2.5 million incidents and $2.4 billion in losses (CloudSEK). Much of this activity has shifted from telco networks to unregulated platforms like OTT communication applications, where traditional security mechanisms fall short.

Spam and fraud are now cross-ecosystem challenges, requiring more than reactive responses.

Because of this, there is a growing need for AI-driven cybersecurity solutions that can deliver real-time detection of phishing links and fraudulent domains received across channels such as SMS, email, OTT messaging, and internet browsing.These systems must not only protect users without disrupting legitimate business communication, but also enable proactive and scalable threat mitigation. Achieving this demands a collaborative approach involving financial institutions, OTT providers, law enforcement, and regulators to build a secure and resilient digital environment.

Solution:

Airtel's Fraud Detection Solution: AI-Led Link Intelligence and Threat Detection

- In May 2025, Airtel launched its **Fraud Detection Solution** – an advanced network-level security solution that protects users from **fraudulent domains and phishing** URLs encountered while browsing the internet or across platforms like SMS, emails and OTT apps (Telegram, WhatsApp, Facebook, Instagram, etc.) in real-time.
- Airtel continuously builds its proprietary database of fraudulent domains by **integrating** data from global threat intelligence databases (Mavenir, Openphish, Mindtest, Google & Microsoft) and is updated every 24 hours.
- When a user clicks on a link, the domain is mapped against this database. If it is identified as fraudulent, it is blocked.
- If the domain is not found in Airtel's database, we use our **partner APIs** to assess it based on several risk markers basis which a **composite fraud score** is calculated in milliseconds and the domain is **blocked at the DNS level** if malicious.
- **Our system connects user interaction signals, AI reasoning engine, and network-level enforcement into one seamless loop**. It is a **modular solution which is easy to integrate with existing telco systems across network and digital interfaces globally**, requiring no transformation and offering rapid time to value.

Impact:

Since its inception, the Fraud Detection Solution has identified and blocked **1,87,154 fraudulent domains**, preventing approximately **30,47,727 fraud attempts daily**, demonstrating not only the importance of this capability but also our deep commitment to user safety.

Additional information

Cost:	Medium
Participating organisations:	airtel
Location:	Asia Pacific

GSMA Head Office
1 Angel Lane
London
EC4R 3AB
United Kingdom
www.gsma.com