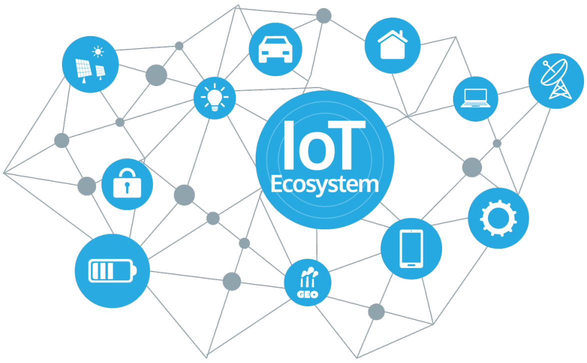
XINTEC
Risk Management. Simplified.

IoT Fraud Detection

The IoT Fraud Detection Challenge

IoT is undoubtably the fastest growing phenomenon in the IT world. We are moving quickly towards a world where any device can connect to the Internet. Today devices as diverse as cars, coffee machines and lightbulbs communicate through the Internet. IoT allows these disparate devices to be married together into fully integrated solutions across a variety of environments.



Communication Service Provides (CSP) have seen IoT as an opportunity to supplement their decline in ARPU. The rapidly growing IoT market is allowing them to secure steady cash flow with minimal added network infrastructure costs. But this expansion has exposed the CSPs to new fraud threats.

There are plenty of opportunities for fraud. Embedded SIMs are often left unattended for long periods, making them more susceptible to tampering; the large number of terminals make them more prone to DoS attacks, or being used to launch such attacks. New provisioning models are likely to create the opportunity for illegal cloning; embedded applications will collect large amounts of personal and private data of great value to fraudsters.

XINTEC's IoT fraud detection solution mitigates these risks. The solution has two modules: IoT Known Behaviour module and IoT Unknown Behaviour module. Both these modules are built on XINTEC's industry proven light-weight core.

IoT Known Behaviour Module

IoT devices often exhibit specific behaviours. These behaviours are encoded into profiles that encapsulate inter-device relationships, location, movement, and activity characteristics of the service. The devices are monitored against these profiles to ensure they behave according to expectations. Alarms are raised against devices or groups of devices that behave abnormally.

Example

An e-Bike fleet will accept financial transactions and report their location every few minutes over a data connection. They will operate within a limited area and only expect to achieve a reasonable maximum speed of 50km/h, for example. The embedded SIMs are fixed to a single e-Bike (meaning there is no change of the IMEI value) and communicate only with the operations support platform.

The characteristics of the e-Bike fleet are encoded into a XINTEC profile. The XINTEC platform monitors the activity of the bikes, raising alarms, e.g.:

- E-bike traveling above reasonable speed threshold indicating it may be carried in another vehicle
- E-Bike movement without associated financial transaction
- E-Bike failed to report location
- Data communication to unsupported APN
- Inappropriate use of communication service

This is a small sample to illustrate the approach of this module. This module supports high grade alarms, clearly identifying violations of the rules, often allowing immediate and automated action.

IoT Unknown Behaviour Module

The second module learns from the behaviour of IMSI groups offering the same service. This module identifies anomalies in IMSI behaviour relative to its peers or anomalies of a group relative to other groups offering the same service.
The module uses advanced clustering algorithms. The module identifies outliers and cluster evolution. Outliers identify individually compromised devices; monitoring cluster evolution helps identify mass compromises and quality issues.

Example

The vehicles of a delivery fleet management service will exhibit groups of similar behaviour. According to the vehicle size, type, and base location the vehicles fall into clusters. Each cluster might exhibit similar distance covered, number and length of stops, operating hours, etc.

When an individual vehicle deviates from its cluster behaviour, perhaps it is rerouting to take on illicit cargo, taking more or longer stops, and adding distance. This behaviour may be detected simply be monitoring deviations from individual normal behaviour, but clusters can identify when multiple drivers collude in these illicit operations as new clusters will evolve.

Anomalies offer insight into suspicious behaviour, but generally require review and analysis before action can be taken. This type of analysis is particularly useful in the context of a managed service, in which the analysis team have the specialist knowledge to tune and interpret analysis.

XINTEC
Risk Management. Simplified.
FMSevolution
IoT Fraud Detection Module
- IOT KNOWN BEHAVIOUR MODULE
- IOT UNKNOWN BEHAVIOUR MODULE
- XINTEC LIGHTWEIGHT CORE

XINTEC Lightweight Core

XINTEC's Light-weight Core (LWC) provides a set of support services to the fraud detection modules. These include the communication module for data:

- Network integration
- Web-based GUI
- Open-source database
- Generic High Usage framework
- Auto-barring & email/SMS alerts
- Standard Reports

The platform utilises Open-source technology: PostgreSQL (SQL DB), Redis (Key/Value store), Python, Java, Apache Tomcat. The fraud detection modules are implemented on the XINTEC Extensible Python Framework (XPF). The XPF is extensible by anyone versed in Python (the world's most popular language) without the need for lengthy development cycles. XPF provides the base services on which the fraud controls are implemented. This platform enables:

- Behavioural profiles management
- Standardised, two-stage analysis allowing complex analysis with minimal resources
- A customer and context data interface
- List management
- Inter-process communication for integration with other fraud modules and external fraud detection environments
- Extensibility with minimal Python knowledge

For further information please contact us: info@xintec.com