bidgely

R & D SERIES

ENERGY THEFT DETECTION TECHNICAL BRIEF

BY THE BIDGELY R&D TEAM

1 INTRODUCTION: SOLVING THE THEFT CHALLENGE

In developing countries, non-technical losses (NTL) have been a growing financial concern for electricity distribution companies. Electricity theft is one of the major contributors to NTL and adversely impacts the profitability of utilities. India plans to deploy 250 million smart meters over the next 3-5 years across the country with an intent to improve billing efficiency, grid reliability, profitability, and customer experience.

In general under AMI infrastructure, smart meters have the capability to record data at 15 min / 30 min / 60 min sampling, which includes energy consumption data, electrical parameters like current, voltage, power factor, etc. along with configured meter events. This granular dataset holds the hidden information of different appliance usage, user's lifestyle, usage behaviour across seasons and related anomalies.

While working with utilities in India on theft detection, we have found that their existing methodologies revolve around analyzing monthly consumption and stand-alone meter events in order to filter down to premises that would have potential for theft. Since these methods do not take into account the appliance-level consumption, usage behaviour and lifestyle factors of premises, we observed that the filtering process is prone to producing a significant number of false positives. Additionally, this method would miss premises showing theft behaviour if the user managed to keep month-level consumption consistent. Additionally, this existing approach involves significant manual work—and therefore is not scalable to millions of premises.

Bidgely, with its advanced AI-based algorithms, has shown success rates in the range of 70-95% for correctly detecting anomalies that resulted in booking 50-60% of energy theft cases by the utility and a strike rate of more than 90% in Tariff Misuse cases.

2 BIDGELY'S SOLUTION FOCUS

In this document we have presented our approach to find premises showing theft behaviour, which has been verified while working with multiple utilities in India. We have leveraged our patented disaggregation algorithms, pattern recognition through behaviour modeling, signal processing and patterns in meter events to find theft premises with high probability. Our solution categorizes theft into four major categories of Tariff Misuse, Direct Theft, Meter Tampering and Sanctioned Load Violations. Through on ground inspection with utilities, we have showcased a high success rate for detecting theft across categories, which has enabled utilities to book the premises and recover financial losses. The following sections discuss Bidgely's theft detection methodology, product capability, proof points for better understanding, and solution data requirements.

One of the striking features of our theft detection product is that it not only provides information about the kind of theft but also its severity and impact on revenue loss, which can help utilities prioritize programs/ visits that not only limit grid-level energy loss but also reduce the operational costs to do so.

Our actionable insights for inspection enable authorities to ensure a high strike/success rate with low turnaround time.

3 THEFT DETECTION METHODOLOGY

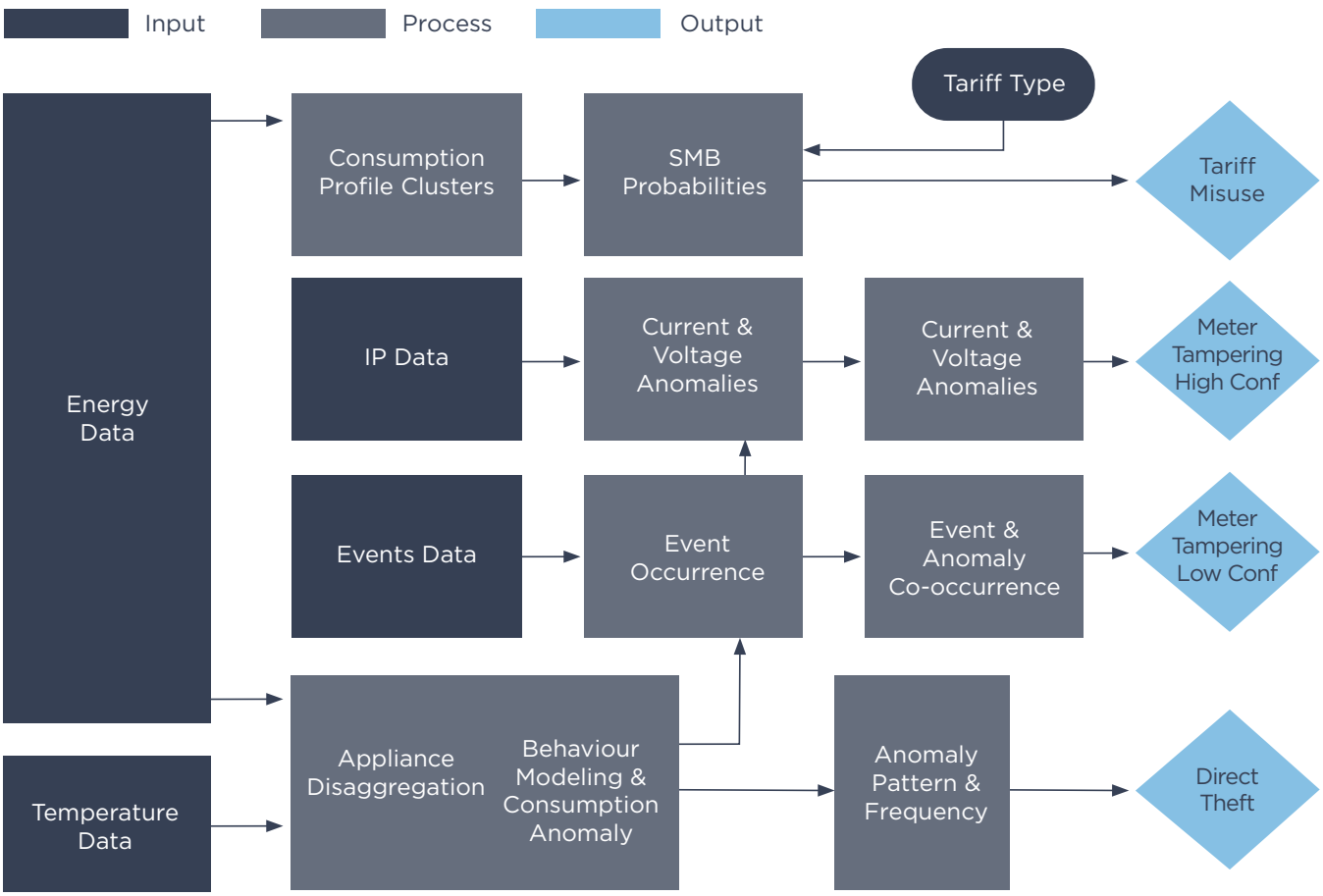

Figure 1: Flowchart for detection of theft categories indicating required inputs, intermediate processes, and outputs.

Our theft detection methodology uses smart meter AMI data provided by utilities, including energy consumption, current, voltage, power factor and non-AMI data like meter events, tariff type (residential, industrial, non-residential, etc.), maximum demand (max power drawn in a bill period), and premises postal code (to get weather data). The "Inputs" blocks in the Figure 1 flowchart represent these inputs.

The core of Bidgely's theft detection methodology—represented in Figure 1 as the "Process" blocks—revolves around behaviour modeling based on AMI data, which leverages information from our patented disaggregation algorithm. This modeling provides information on behavioural anomalies for the premises. Further, the anomalies are extracted out of current and voltage data and correlated with meter events and behavioural anomalies to classify premises for direct theft or meter tampering.

For tariff misuse, consumption profiles from energy consumption data are built and further processed through a trained clustering model to classify premises for non-residential activity. This information is then grouped with tariff type to classify premises for tariff misuse.

The outputs of this method—Figure 1 "Output" blocks—include theft category classes, the loss incurred to utility, theft probability, and actionables to help authorities conduct effective on-ground inspection.

4 THEFT CATEGORIES

Based on the data patterns found in smart meter data, our theft solution identifies and classifies the theft premises under four broad categories. These categories are: Tariff Misuse, Direct Theft, Meter Tampering and Sanctioned Load Violations. The subsections below describe each category in detail.

4.1. Tariff Misuse

In general, rate plans offered by utilities differ for domestic (residential) and non-domestic (commercial) premises, with non-domestic tariffs usually higher than domestic ones. While working with utilities, we have come across cases where premises are registered under domestic plans but are using their connection for electricity for commercial activity such as shops, offices, commercial/manufacturing units, schools, machinery, construction sites, etc. Though there is no energy loss to utilities in such cases, there is a revenue loss to utilities on account of the differential in tariffs. This revenue loss can be large and perpetual in a population of millions of premises across months. Bidgely's UtilityAI™ algorithms accurately identify non-residential activities based on the consumption patterns in AMI data. Our solution is capable of identifying not just residential and non-residential behaviours but also premises with mixed use.

Exhibit A: Purely commercial usage

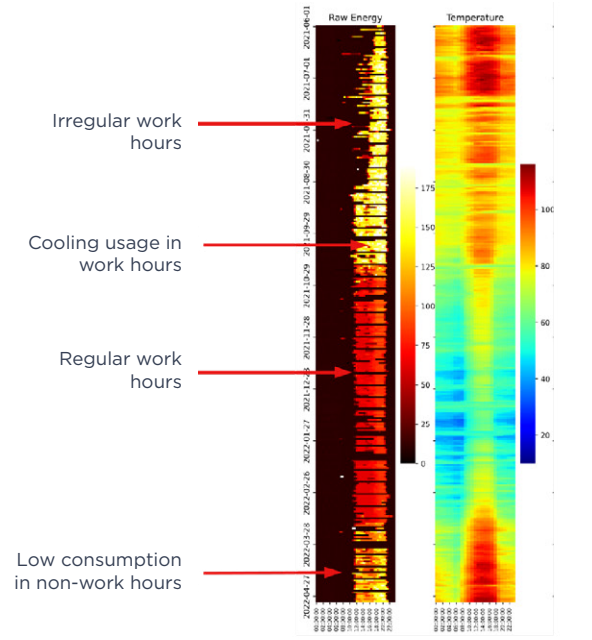

Exhibit B: Commercial usage within residential premises

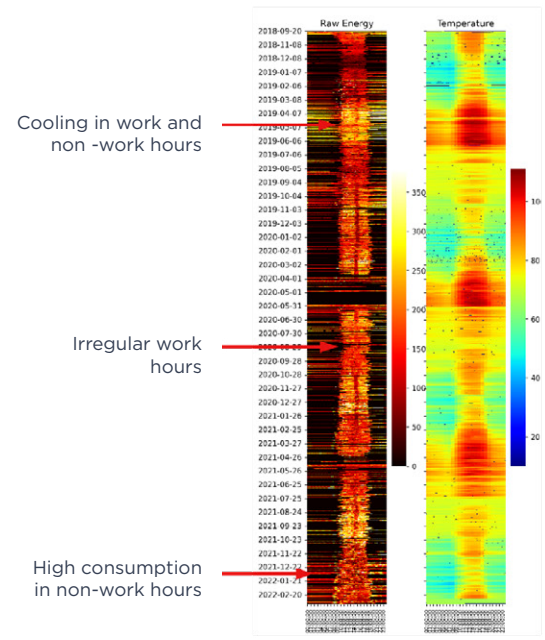

Figure 2

In Figure 2, Exhibit A shows the consumption pattern from a meter under a residential tariff. This pattern reflects the presence of purely commercial behaviour. On the other hand, Exhibit B shows a consumption pattern of mixed residential and commercial activities. The two exhibits were flagged for tariff misuse by the algorithm, with commercial activity from hours 12:00 to 22:00 for Exhibit A and hours 10:00 to 17:00 for Exhibit B. The on-ground inspection on the reported premises revealed Exhibit A to be an office and Exhibit B to be a residential premises where commercial machinery was being used in the basement. This example depicts the robustness of AI algorithms for spotting not just easily identifiable tariff misuse cases but also the ones with complex energy usage patterns.

4.2. Direct Theft

While working on theft detection with utilities in India, Bidgely encountered cases where end consumers of electricity found ways to bypass the smart meters so that consumption did not get recorded in the meter, either partially or completely. Direct theft can vary from night theft, day theft, intermittent theft across multiple days, appliance bypass, etc. Our algorithms are able to identify premises by characterizing direct theft behaviour. It is extracted using energy disaggregation and the energy consumption pattern of the premise, user lifestyle and weather information for the location.

Common ways of indulging in direct theft include: splitting the service wire, using a switching mechanism, hooking into transformers or LT poles especially when they are located near the premises, etc.

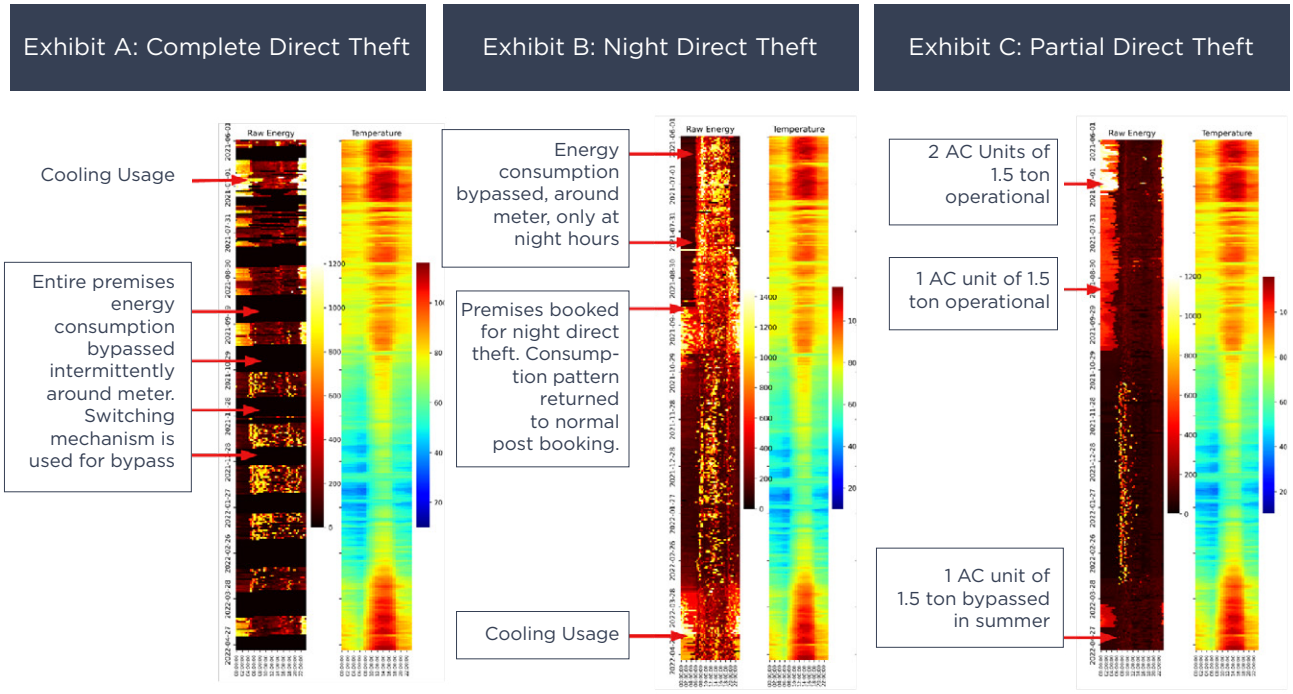

Figure 3

In Figure 3, three energy consumption exhibits are shown that were identified by our algorithm as direct theft while working with an Indian utility. Exhibit A shows the entire premises' energy consumption is being bypassed intermittently. This method is used to keep overall monthly consumption consistent, which makes it difficult for the utility to point out theft behaviour by analyzing only the monthly consumption. Bidgely's UtilityAI™ algorithm can spot such cases accurately. The on-ground inspection for this incident revealed a switching mechanism was being used for direct theft. Exhibit B shows direct theft behaviour being carried out only during night hours. After the user was booked for night theft, the consumption pattern returned to normal. Exhibit C shows that AC usage was consistent in the summer of 2021 where evidently two AC units of 1.5 tons each were in use at different times. In 2022, AC usage reappeared with the onset of summer, but as summer temperatures started peaking, AC usage was bypassed from the meter while there was occupancy at the house.

4.3. Meter Tampering

Another way in which the actual energy consumption happening at a residence or business does not get reflected in meter data is when the meter itself is tampered with. For example, if a shunt or wire is illegally installed within a meter the actual energy consumption may not be reflected. There are various other cases of meter tampering that are of interest, such as cover open, terminal burnt, effect of external magnetic device, etc. Bidgley has devised a set of algorithms that leverages energy consumption patterns, technical parameters of phase currents, neutral currents, voltages, power factors and available smart meter events in order to identify meters where tampering is most likely to have taken place.

Exhibit A: Meter tampering case based on derived event from current and voltage derived consumption anomaly from behaviour analysis

Exhibit B: Meter tampering case based on derived event from current and voltage, direct meter event and derived consumption anomaly from behaviour analysis

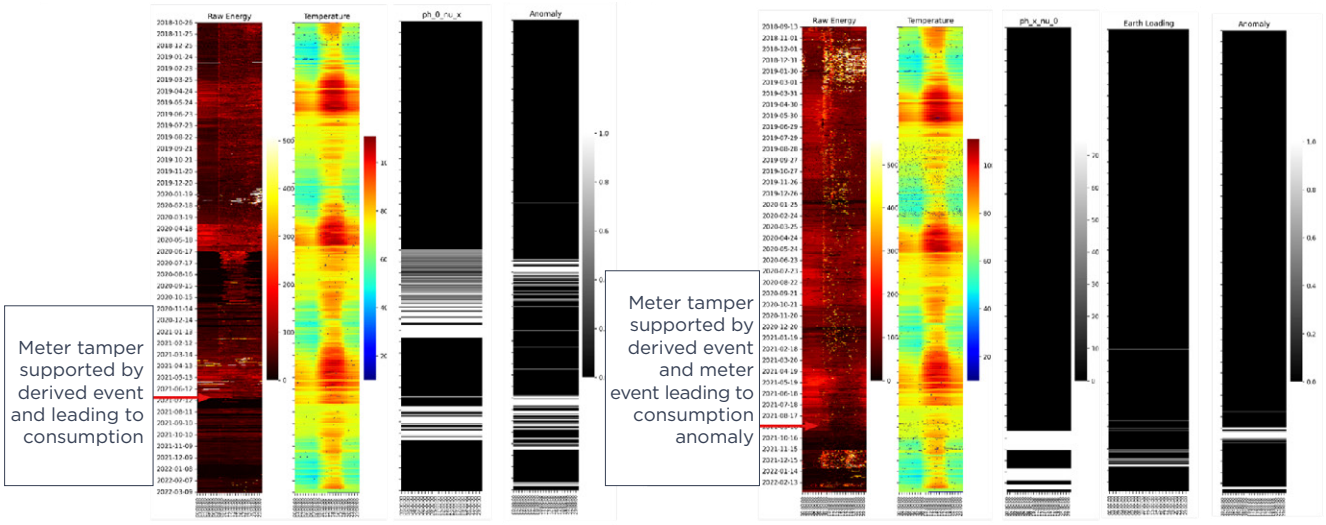

Figure 4

In Figure 4, Exhibits A and B show two meter tampering cases. In Exhibit A, the third heatmap from left shows a derived event based on AMI phase current, neutral current and voltage. The furthest right heatmap shows consumption anomalies found through behaviour modeling. It can be observed that the coherence of consumption anomalies and derived events across days, giving confidence that Bidgely's UtilityAI™ algorithm is able to accurately flag the premises for meter tampering. Likewise in Exhibit B, in addition to the derived event, the coherence of a direct meter event with consumption anomaly gives higher confidence with regard to flagging the premises for meter tampering.

In addition to these examples, there are other meter tampering cases such as terminal burn, cover open, current without voltage, etc. that are of interest to utilities and do not necessarily have a consumption anomaly co-existing with the events. Such cases are identified and reported as they occur in data.

5 THEFT QUANTIFICATION & ACTIONABLES

Bidgely's theft detection solution not only identifies the kind of theft—meter tampering, direct theft, or tariff misuse—but also specifies the severity of the loss and its impact on revenue.

This additional insight enables utilities to prioritize their operations and methodologies related to site visits or issuing warnings to consumers, reducing operational costs on account of field visits, man hours, targeting cases with best ROI etc. Result outputs include:

1. **High-, Medium- and Low-Probability Lists of Suspects -** A probability score is assigned on the basis of severity and persistence of anomalous behaviour. Though high-probability cases require immediate action, medium- and low-probability cases are also significant and should be kept under close watch as their propensity for engaging in theft could negatively impact billing efficiency and, more importantly, customer safety.
2. **Actionable Reports -** Focused reports explain anomalies and define the 'what,' 'where,' 'when,' and 'how' elements of inspection.
3. **Quantification of Loss to Utility -** Prioritization on the basis of estimated losses in terms of energy and costs help the energy provider prioritize their action for cases causing higher losses.

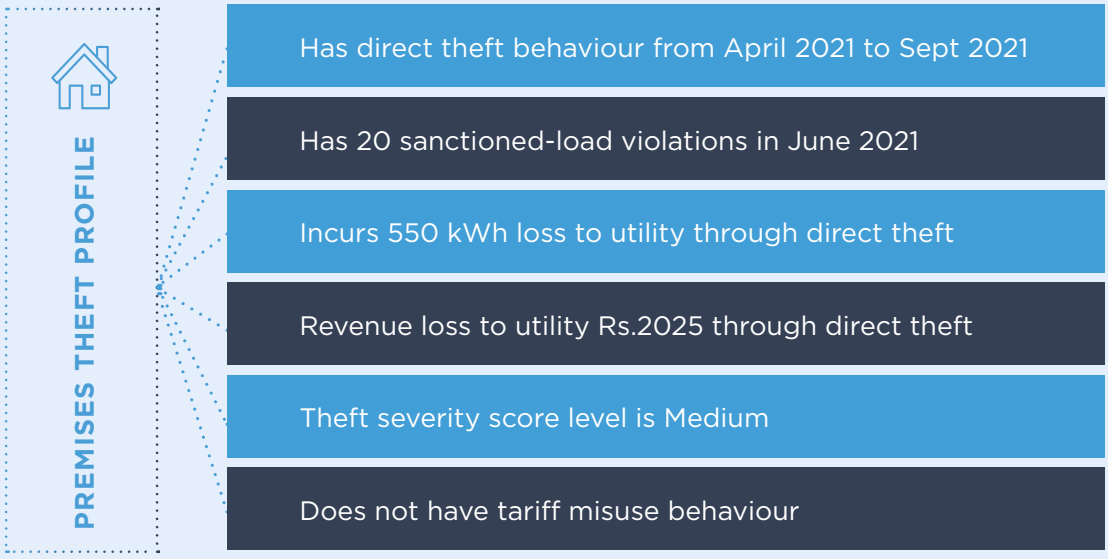

Figure 5: Sample Premises Theft Profile showing quantification of loss due to theft behaviour detected at the premises.

6 DATA REQUIREMENTS

In order to do effective theft detection, at least nine months of AMI data and meter events (mentioned in tables below) are required for single-phase and three-phase meters.

Furthermore, since tariff misuse depends solely on consumption profiles, a minimum of four months of meter data is required for processing and profile classification, which improves as months of data availability increase.

Because meter bypass, night theft, and direct theft do not depend on meter events, a minimum of four months of data is required if theft behaviour is shown within this data duration, and this detection also improves with each additional month of data.

For remaining theft types, seasonal behaviour modeling is essential and requires at least nine months of data to cover summer and winter behaviours and detect pattern changes across seasons. Details for these data requirements are provided in the tables below.

1 Phase Meters	AMI Level Data (at data sampling level)	Energy consumption (Wh)	
		Average phase current (A)	
		Average neutral current (A)	
		Average phase voltage (V)	
		Power factor (unitless)	
	Instantaneous Meter Events	Earth loading event	External Magnet event
		Cover open event	Current mismatch event
		Neutral lost event	Single wire operation
		Current unbalance	Current Bypass
3 Phase Meters	AMI Level Data (at data sampling level)	Energy consumption (Wh)	
		Average phase current (A): All 3 phases	
		Average neutral current (A)	
		Average phase voltage (V): All 3 phases	
		Power factor (unitless): All 3 phases	

3 Phase Meters	Instantaneous Meter Events	CT bypass event	External magnet event
		Cover open event	Voltage missing event
		CT open event	Voltage unbalance
		Current unbalance	Earth Loading
		Low power factor	Neutral disturbance

Apart from AMI data, other required information is mentioned in the table below, which falls under a non-AMI / static data type category.

Non-AMI / Static Data	Sanctioned Load (kW)	Sanctioned load of meter as per record
	Maximum demand (kW)	Maximum power drawn at bill cycle level or at whichever level it is available
	Tariff category	Domestic/Non-domestic/Industrial/ Agricultural tag
	Zip Code	Postal zip code of meter's premises
	Billing data	Bill cycles of meter

The above mentioned nine months data duration is the requirement across all categories of theft. The category data requirement is mentioned in the table below.

Theft category	Sub category	Minimum duration requirement
Tariff Misuse	N/A	4 months data
Direct Theft	Complete meter bypass	4 months data
	Partial meter bypass	9 months data
	Night theft	4 months data
Meter Tampering	1. Special Event: Cover Open 2. Special Event: External Magnet 3. Current without voltage 4. Terminal Burnt: Voltage missing	No minimum requirement, If evidence is present in provided data
	Shunt or related tampering	9 months data

Given the dataset duration, if evidence of a theft category is detected in the dataset, theft cases will be reported.