bidgely

BIDGELY'S AI-POWERED ENERGY THEFT DETECTION SOLUTION

A SMARTER, MORE RESILIENT GRID

In the next 3-5 years, India plans to deploy 250 million smart meters in its bid to strengthen the energy distribution sector. A key objective of this effort is to significantly reduce the level of non-technical losses, which will improve grid reliability, power quality, customer safety, utility profit, and customer experience.

Smart meter data holds the key to theft reduction—which is anticipated to deliver more than ₹790 billion (USD10B) in savings annually in the country. But smart meter data alone cannot provide the insights needed to take action against losses.

A BETTER WAY FORWARD

Historically, apart from basic meter hardware tamper alerts, broad-scale theft detection has been a top-down approach implemented at the grid level. This high-level view, however, is limited to assessing groups of homes associated with a single substation—for example, the 100,000+ homes on a particular feeder/substation—and flagging that group for review. The resulting investigation process can take weeks or months of effort to resolve in the field.

But Artificial Intelligence (AI) can process more data much faster for all homes—in hours, not days—and, like a detective, provide a clear, data-driven picture of exactly what is happening behind each meter, so the utility has specific information about each meter and home to act on.

AI vs. Statistical Analysis

1. AI can process large amounts of data for each meter individually.
2. AI can analyze the consumption patterns of each user over a longer period of time. Statistical Analysis is limited to a segment of time—for example, one month—and could miss important consumption trends.
3. AI can correlate and superimpose many different variables to highlight anomalies in various categories at the same time—for example, multiple technical and commercial parameters.

Bidgely's Energy Theft Detection Solution is built on AI capabilities in development for more than a decade.

Bidgely's UtilityAI™ Energy Theft Detection Solution lets utilities discover, understand, and remedy theft quickly by taking detection right down to the individual home and looking behind the meter to discover tariff misuse, direct theft, and/or meter tampering.

SMART DETECTION FOR DIFFERENT TYPES OF THEFT

1 TARIFF MISUSE

Tariff Misuse occurs when a customer's electricity use type is mischaracterized, and an incorrect lower tariff is applied. For example, where a connection is being billed as a residential customer but in reality is being used for commercial purposes, such as to operate a shop, coaching center, construction site, machinery, or similar enterprise.

Bidgely's UtilityAI™ algorithms accurately distinguish between residential behaviour and commercial behaviour, and also identify patterns indicative of commercial activity on a residential tariff, including more challenging situations where there is mixed use.

2 DIRECT THEFT & ANOMALOUS BEHAVIOUR

Direct Theft & Anomalous Behaviour occurs when a consumer partially or completely bypasses the meter using an illegal connection mechanism to power some or all appliances. For example, consumers may "hook" distribution lines through wires, cables, etc. in order to place the meter in or out of circuit so that actual consumption is not recorded.

Bidgley's patented energy disaggregation algorithms detect several categories of **consumption anomalies** and energy use behaviour patterns, including:

1. Permanent bypass of select appliances - The anomaly is extracted based on sanctioned load, occupancy, and/or lifestyle profiling.

2. Intermittent bypass of select appliances - The anomaly is extracted based on appliance ownership, lifestyle, occupancy, and usage profiling.

3 METER TAMPERING

Meter Tampering occurs when the meter itself is tampered with to prevent consumption from registering. Examples include:

- Installing a shunt within the meter to "jump" the connection between grid supply and premises wiring
- Changing the sequence of terminal wiring
- Changing current transformer ratio to reduce the recorded consumption
- Phase-to-phase short circuit
- Using alternate neutral lines

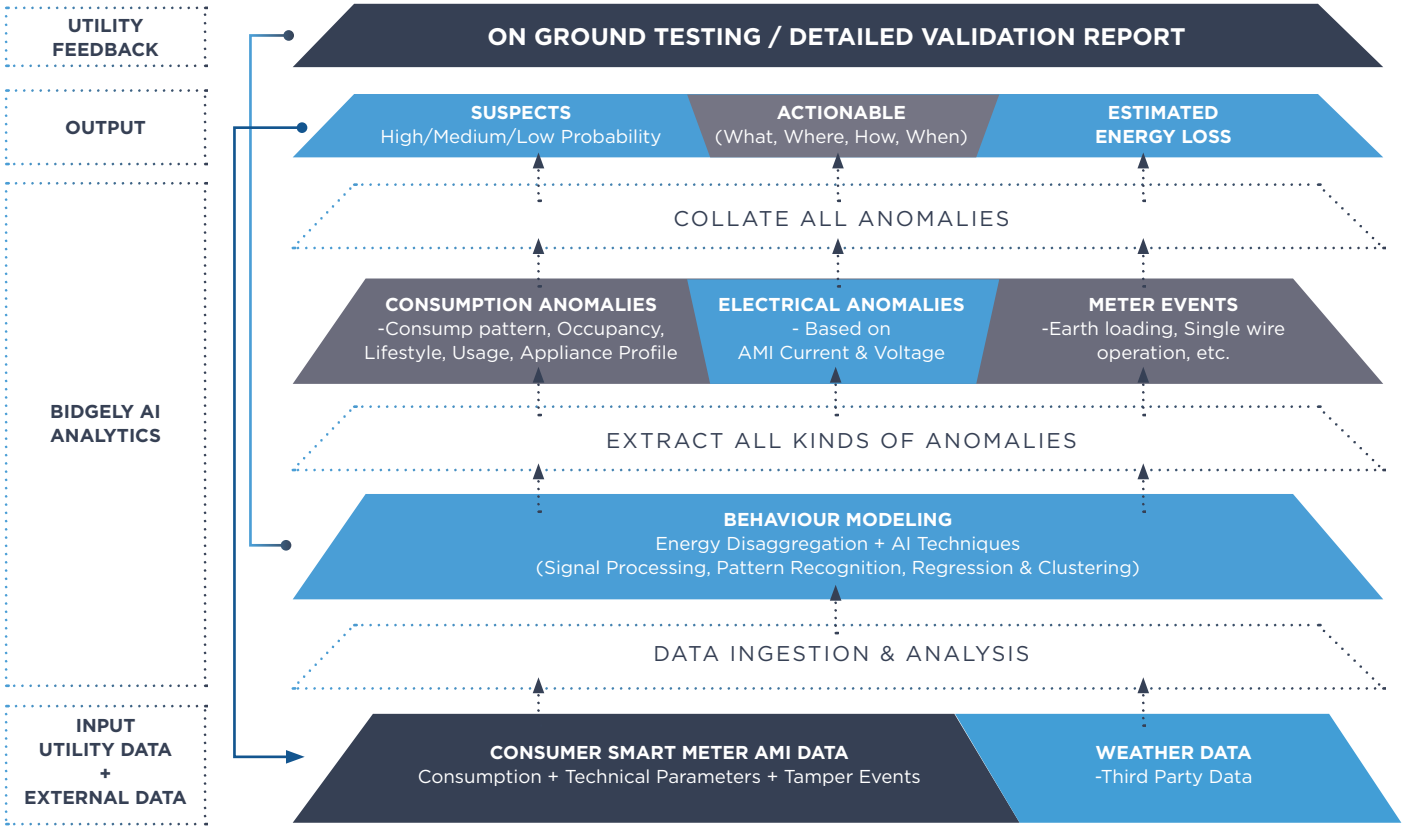
Bidgely's UtilityAI™ algorithms leverage energy consumption patterns, technical parameters of phase currents, neutral currents, voltages, power factors and available smart meter events to identify premises where meter tampering is most likely to have taken place.

BIDGELY'S UTILITYAI™
ENERGY THEFT DETECTION SOLUTION

Bidgely's AI-based analytics—backed by 17 energy-specific data science patents—center on dissecting **consumption data**. Any anomaly in consumption can be understood by analyzing consumption patterns through a toolset that includes signal processing, pattern recognition, regression and clustering techniques, and unsupervised algorithms—which enables Bidgley to detect anomalies on the fly without any ground truth requirement for theft cases from the utility end.

An important distinction in Bidgley's approach is that our methodology assigns a **theft probability** score to non-sanctioned activity to determine the likelihood of a customer engaging in theft as well as a quantification of estimated losses. This score enables energy providers to prioritize their efforts and optimally utilize resources for targeted handling of cases, beginning with those with the best potential ROI.

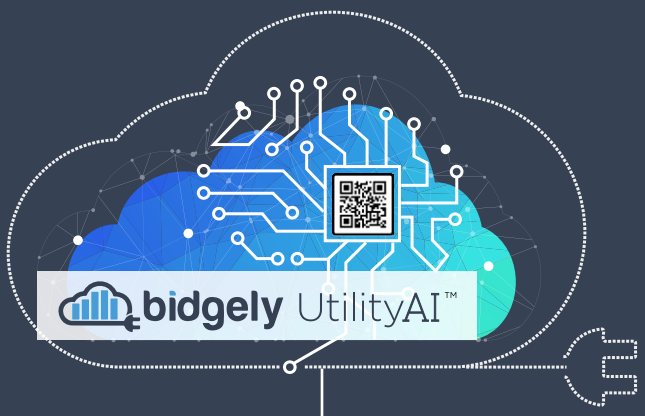
BIDGELY'S APPROACH



STEP 1: DATA INGESTION

Bidgely ingests granular smart meter data—including consumption, current, voltage, meter events, power factor, and MDI—as well as additional external data including weather, geography, and demographic data into our AI processing suite to analyze for occupancy, lifestyle profile, consumption pattern, and presence of heavy loads such as heating and cooling.

Bidgely can work with raw meter data files in the absence of pre-processing by a Meter Data Management System, conducting quality checks on the data and identifying useful meter events and instantaneous parameters such as current, voltage, and power factor. These insights are formatted and processed along with consumption data to provide clean, multi-factor data for the following analysis stage.



Consumption Anomalies

Electrical Anomalies
AMI Current & Voltage based

Meter Events
Earth loading, Single wire operation, etc.

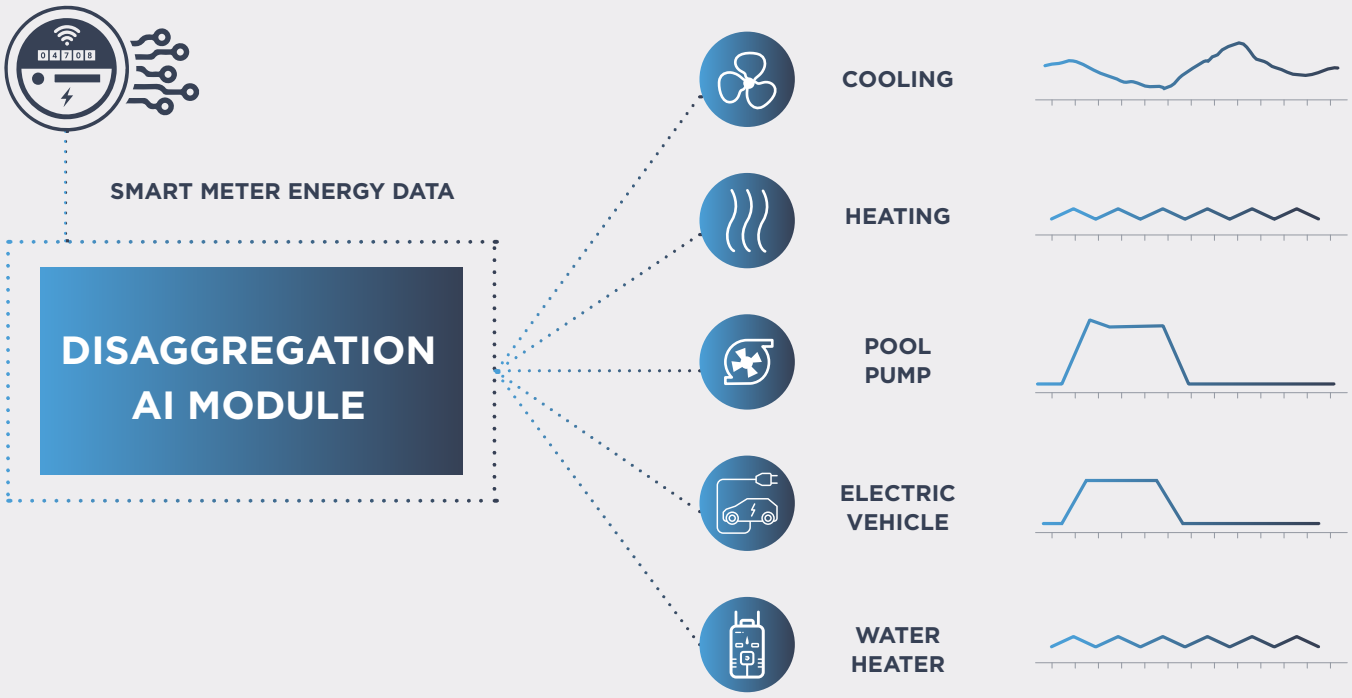
Weather data/ Other External Factors

STEP 2: ANAYLSIS

Bidgely's theft analysis solution is built on four AI modules that process the ingested data like a human brain, looking for patterns and relationships within the data to deliver a comprehensive picture of theft.

MODULE 1: ENERGY DISAGGREGATION

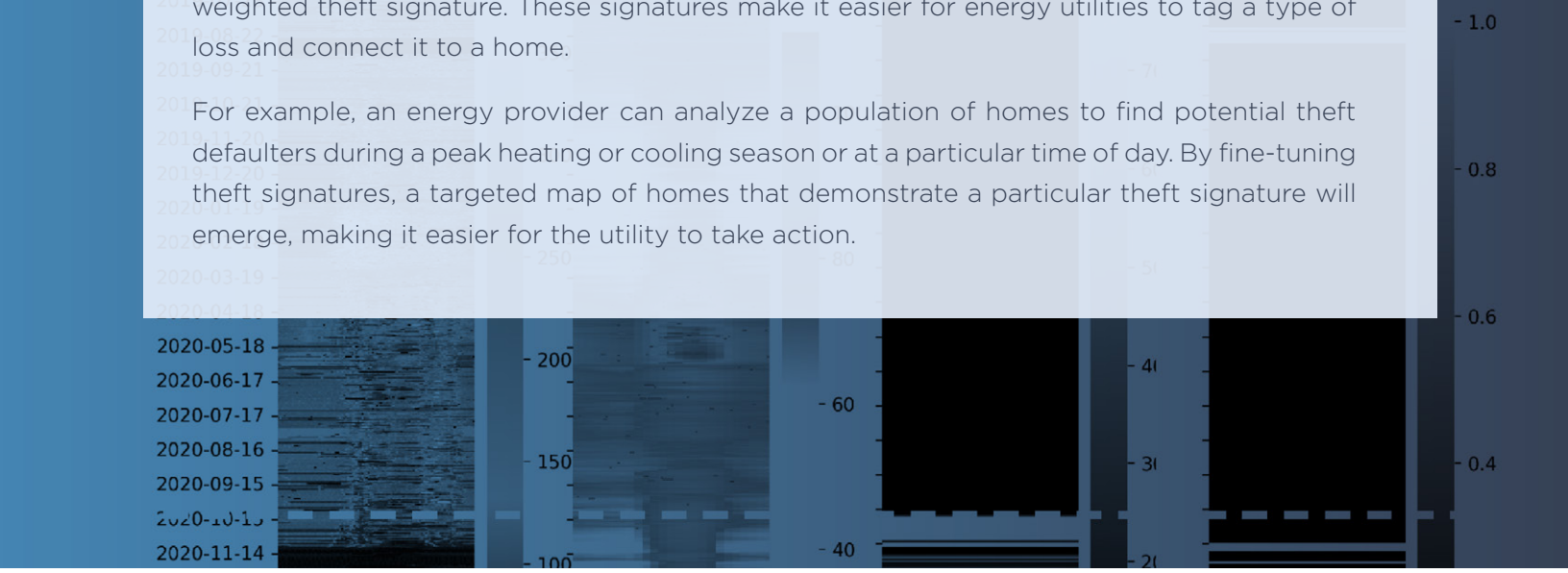
Our patented disaggregation algorithms identify consumption by specific appliance type. Our algorithms can also determine when an appliance is running and how much energy it is consuming. The disaggregated appliance energies and their attributes are fed into the theft AI suite.

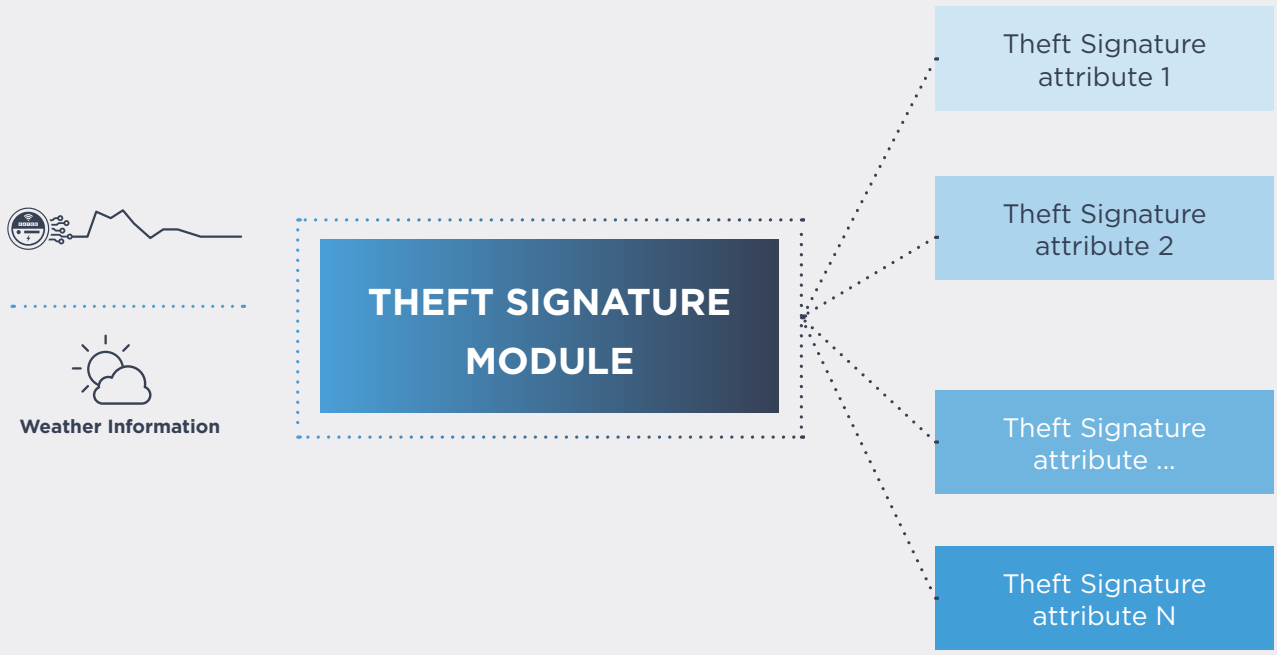


MODULE 2: IDENTIFICATION OF THEFT SIGNATURE PATTERNS

The Theft Signature Module ingests smart meter data along with weather data. It then implements a set of machine learning and pattern recognition algorithms to model expected behaviour within each day. Deviations from normal consumption behaviour are assigned a weighted theft signature. These signatures make it easier for energy utilities to tag a type of loss and connect it to a home.

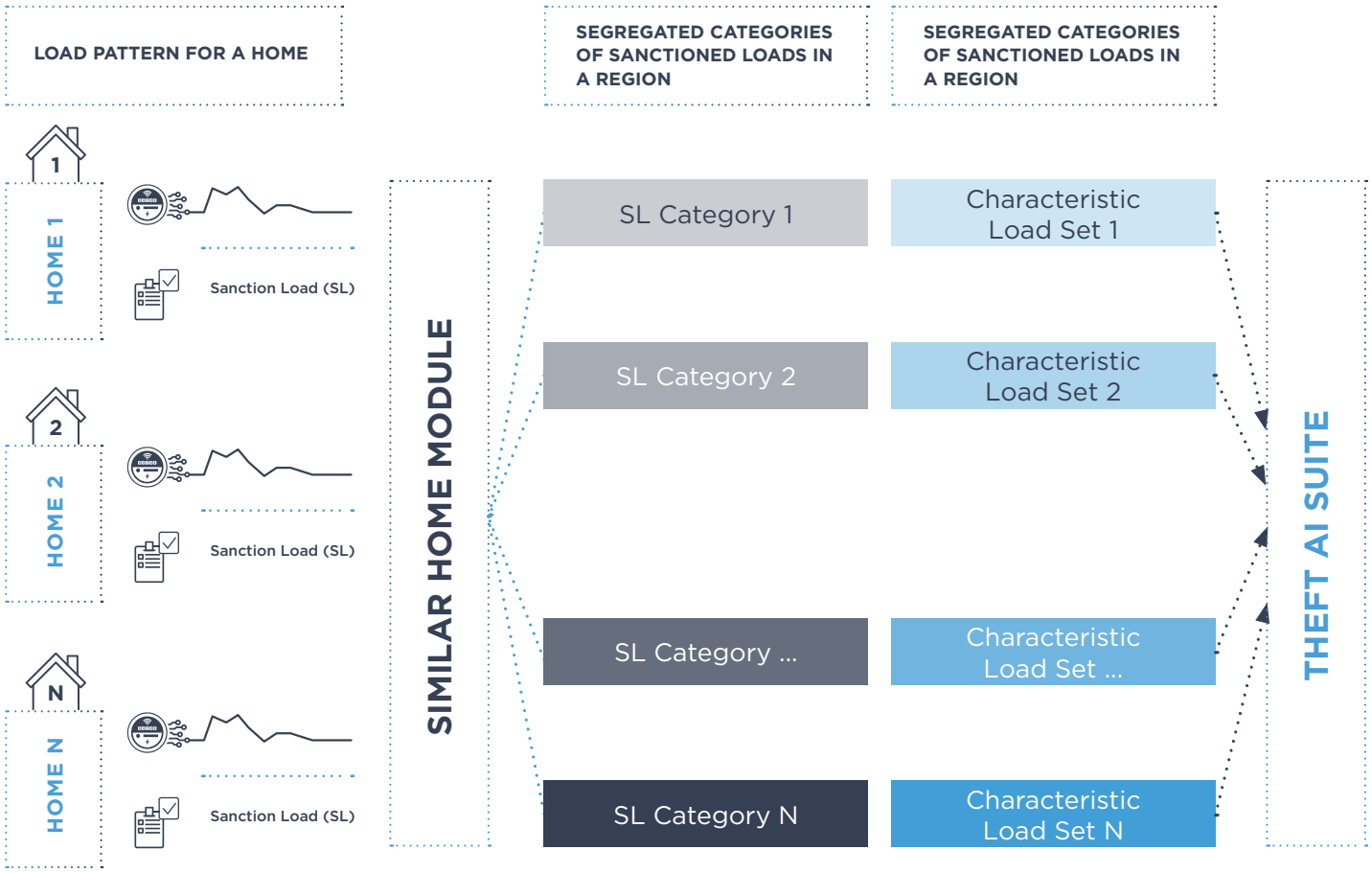
For example, an energy provider can analyze a population of homes to find potential theft defaulters during a peak heating or cooling season or at a particular time of day. By fine-tuning theft signatures, a targeted map of homes that demonstrate a particular theft signature will emerge, making it easier for the utility to take action.





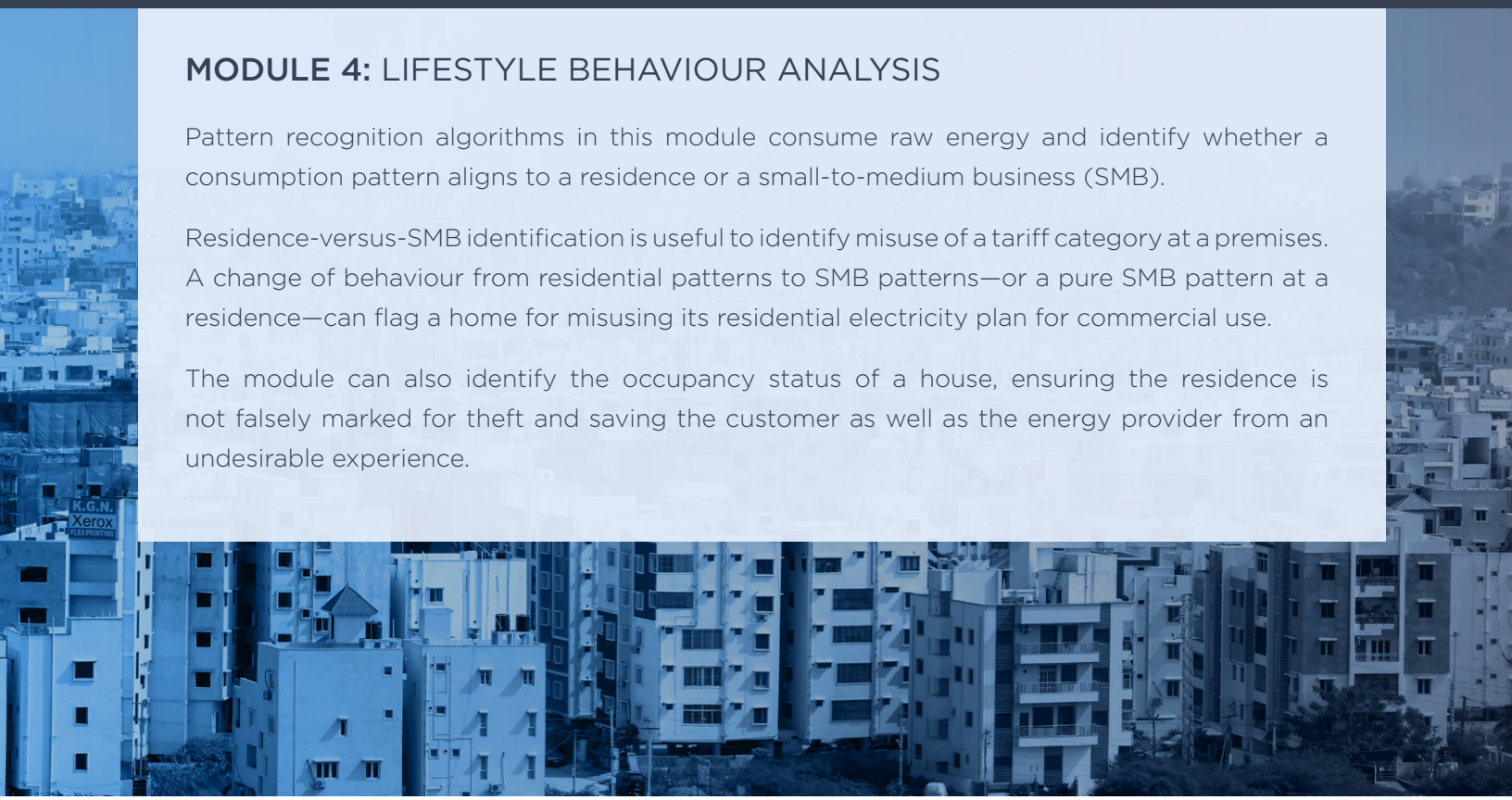
MODULE 3: SIMILAR HOMES COMPARISON

We then analyze energy consumption and sanctioned load across a population of homes in order to run a comparative analysis across a set of sanctioned load categories to identify violators within a population. For example, if a home shows a bypass in consumption during the summer when similar homes in the area do not, a utility can precisely target the marked home for corrective action.



SL: Sanction load for maximum power drawn for a house, set by utility at time of meter installation, based on appliances present in a home.

Characteristic load: Load pattern set for a similar sanction load category that signifies the expected load variations for that sanction load type.

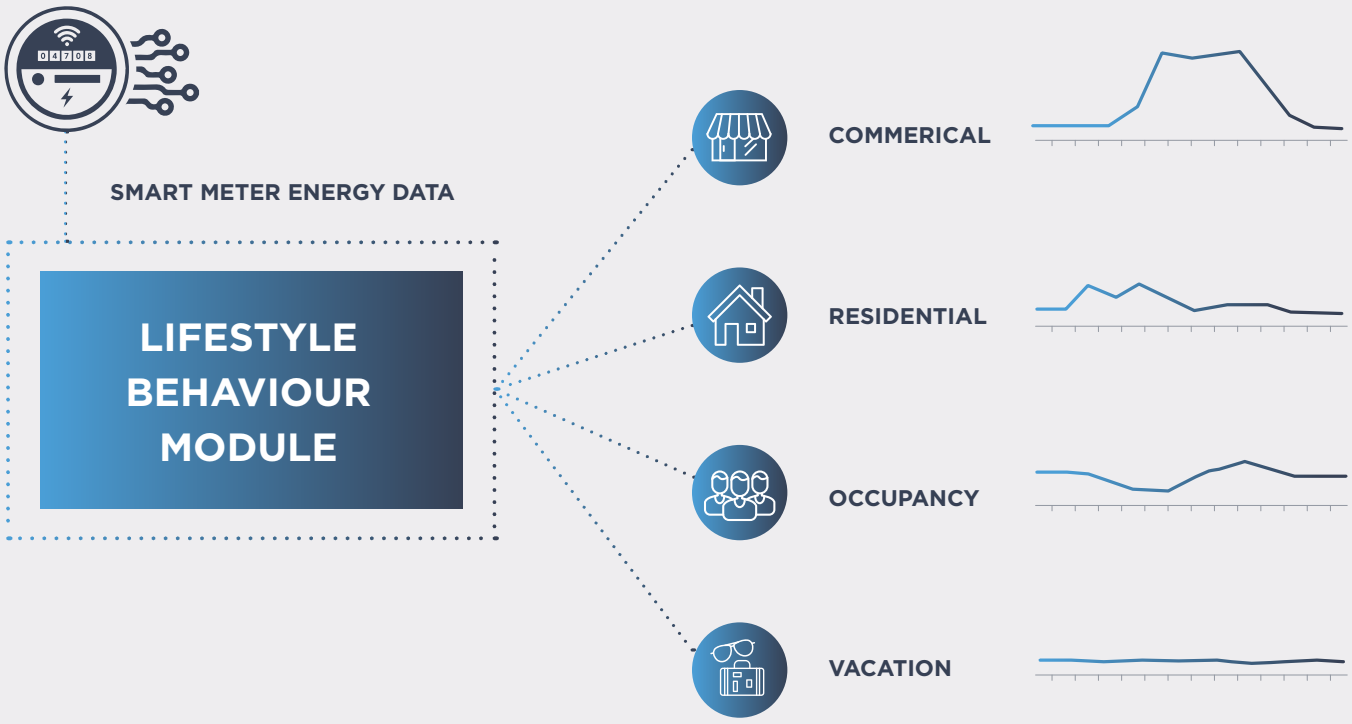


MODULE 4: LIFESTYLE BEHAVIOUR ANALYSIS

Pattern recognition algorithms in this module consume raw energy and identify whether a consumption pattern aligns to a residence or a small-to-medium business (SMB).

Residence-versus-SMB identification is useful to identify misuse of a tariff category at a premises. A change of behaviour from residential patterns to SMB patterns—or a pure SMB pattern at a residence—can flag a home for misusing its residential electricity plan for commercial use.

The module can also identify the occupancy status of a house, ensuring the residence is not falsely marked for theft and saving the customer as well as the energy provider from an undesirable experience.



STEP 3: QUANTIFY & QUALIFY RESULTS

Once the analysis is complete, 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 value assignment enables utilities to prioritize programs and verification visits that deliver greater grid value with more accuracy and speed.

Results outputs include:

1. **High-, Medium- and Low-Probability Lists of Suspects** — The probability score is assigned on the basis of severity and persistence of anomalous behaviour in the recent period. 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 of energy help the energy provider prioritize high-loss customers for intervention.

Each account flagged for potential theft is given a profile based on these results.

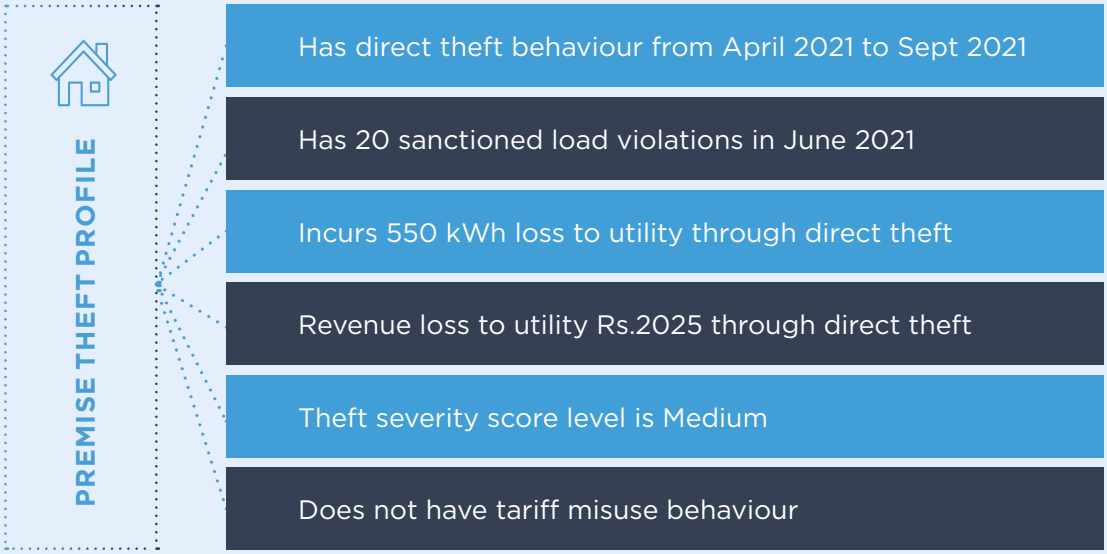


Figure 5: Figure shows quantification of loss because of theft behaviour detected at a premise.

THE NEW STANDARD

Premises-level energy theft detection enabled by artificial intelligence is setting a new benchmark for theft detection. As the leader in energy disaggregation, with 17 patents and experience working with over 40 utilities serving 25 million homes worldwide, Bidgely is applying its "Energy Intelligence" capabilities to the theft challenge, enabling utilities to not only see and understand loss with precision and accuracy but also evaluate its severity and impact on revenue loss. The result is potentially unprecedented benefits to utility revenue, grid performance, customer experience and safety.

GETTING STARTED

Bidgely's Energy Theft Detection solution helps energy providers look behind the meter to determine exactly what appliance-level energy usage is occurring in every home and then equip those providers with precision intelligence tools to discover, understand, and remedy theft quickly.

To learn more about how Bidgely can help you successfully combat theft, visit www.bidgely.com/solutions/energy-theft-detection, or contact a representative at **utilityai@bidgely.com**.

bidgely