
ELECTRICITY
THEFT
DETECTION
KES
FIGHTING POWER THEFT WITH AI

Meet the Group Members

Sharon Thiga

Victor Wasuna

Github Name

Joan Omanyo

Github Name

Kelvin Sesery

Github Name

Elizabeth Gichure

Github Nme

Ann Wahu

Vincent Buluma

Github Name

The Team

Sharon Thiga

Ann Wahu

Joan Omanyo

Elizabeth Gichure

Victor Wasuna

Kelvin Sesery

TABLE OF CONTENTS

1

BUSINESS UNDERSTANDING

Business Problem

Electricity theft costs global utilities $96 billion annually and reaches 20-40% of revenue in emerging markets like Kenya.

These losses inflate tariffs for honest customers and destabilize electricity grids. Our motivation is to leverage data science to combat this corruption, making electricity more affordable and reliable

Industry & Audience

Targeted at electricity distribution utilities (e.g., Kenya Power, Eskom) and energy regulators who are responsible for ensuring grid stability and fair billing.

Stakeholders

- Primary: Utility companies (finance, operations, investigation teams)
- Secondary: Energy regulators, policy makers, and honest electricity consumers
- Indirect: Investors and technology partners interested in AI for social impact

Impact

Deploying this AI system could reduce electricity theft losses by 30-50%. Unlike previous research on load forecasting, this project applies predictive modeling to detect electricity theft, combining real consumption data with synthetic theft patterns based on IEEE research, filling a critical gap in the literature and practice.

1

MAIN OBJECTIVE

Early Accurate Theft identification

Develop a predictive model capable of detecting electricity theft with high recall, ensuring that the majority of theft cases are identified early and minimizing missed violations. Target of F2-Score> 0.70

Operational Efficiency and Revenue Protection

Leverage model predictions to optimize inspection resources by prioritizing high-risk customers, thereby maximizing the financial impact of field investigations.

Precision@K to ensure inspections focus on the most suspicious accounts

Estimated financial savings (KES billions) to quantify tangible business value

Explainable, Decision-Centric Deployment

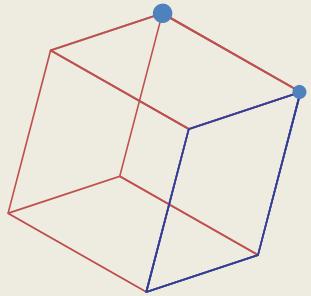
Implement an interactive Streamlit-based dashboard that translates model outputs into clear, actionable insights for utility investigators and decision-makers.

2

DATA UNDERSTANDING

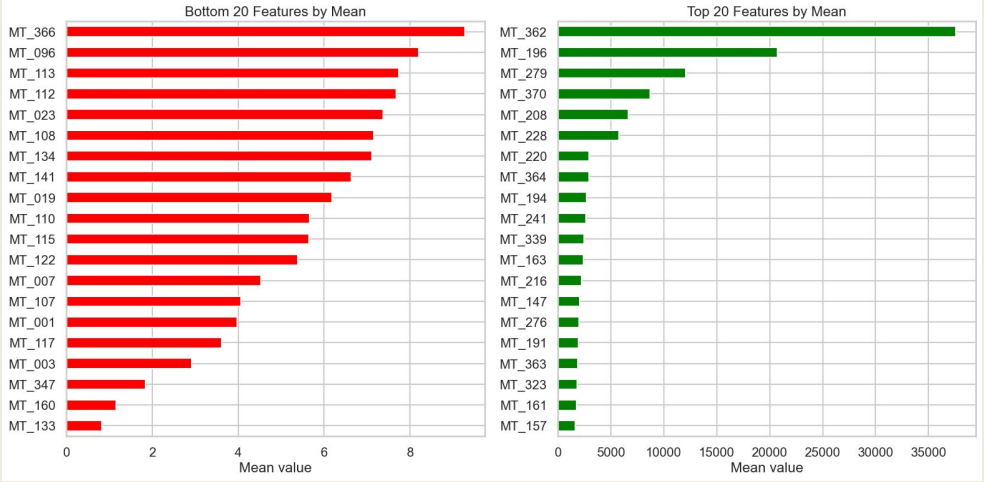
Key Understanding required

- Individual meter behaviour
- Distribution of Electricity per meter
- Electricity consumption distribution
- Time patterns for meter
- Average electricity consumption per day, week and month
- Discovering patterns and cluster by use by Elbow and K mean Clusters



2

DATA UNDERSTANDING



Asymmetry in Means:

The top 20 features (green, right panel) have extremely high mean values, with the highest around 35,000–40,000.

The bottom 20 features (red, left panel) are much smaller, mostly below 10.

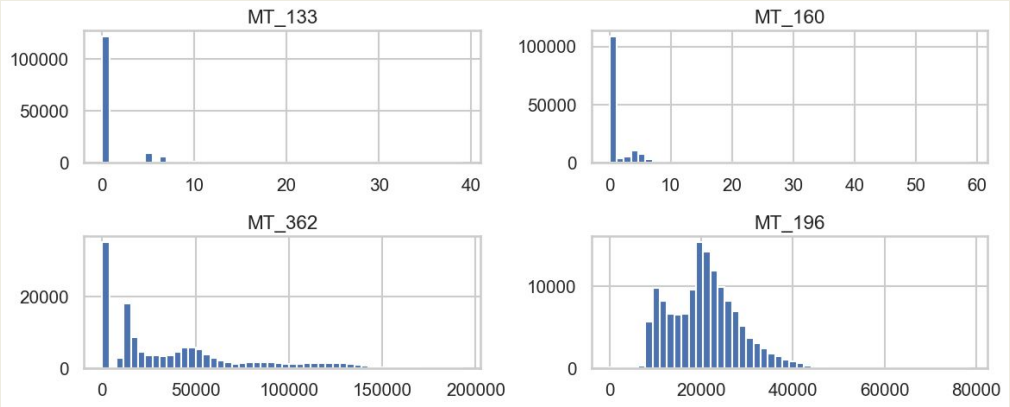
This suggests a highly skewed distribution, likely a few customers/meters dominate the overall consum extremes.
Insights:

The top features might represent heavy or high-usage meters, possibly outliers or industrial customers.
Bottom features could indicate low usage or less active meters, possibly residential.

The distributional analysis reveals two distinct consumption regimes.

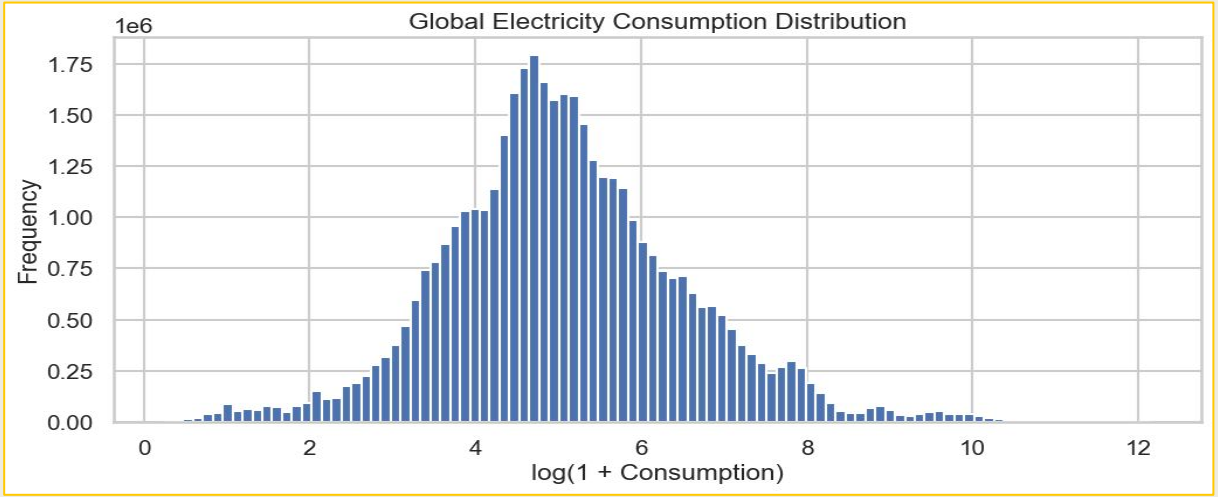
MT_133 and MT_160 show highly concentrated low-usage patterns,

MT_362 and MT_196 exhibit heavy-tailed, high-variance behavior.



2

DATA UNDERSTANDING



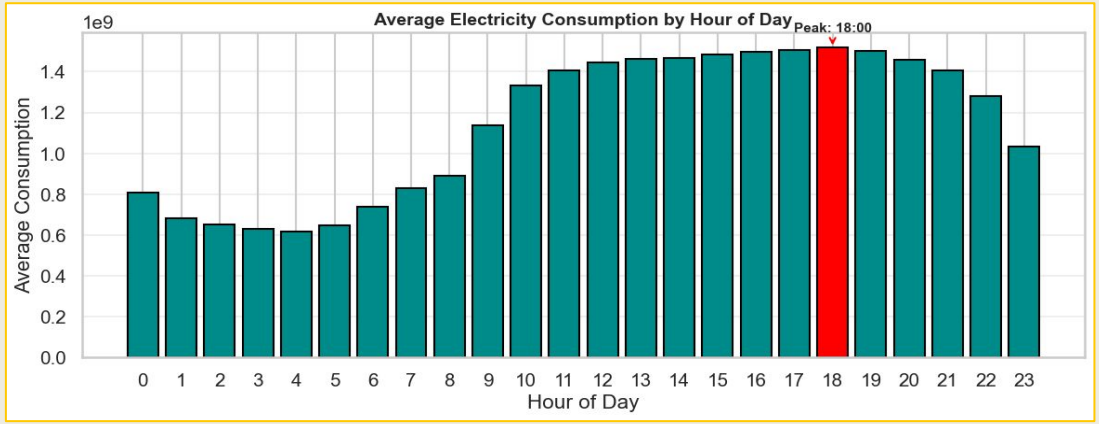
We are justified in using a single global model because:

The population does not exhibit clear multimodality after log transformation.
Differences between low-, medium-, and high-consumption users form a continuous spectrum rather than discrete groups.
Applying clustering would introduce artificial segmentation not supported by the underlying data distribution.

Deduction on hourly pattern

Demand is lowest around 02:00–05:00, rises sharply after morning hours, and peaks between roughly 16:00 and 19:00 before slightly declining at night.

This intraday profile is typical of residential and commercial usage, with higher activity and appliance use in late afternoon and early evenings



DATA PREPARATION

Key Activities

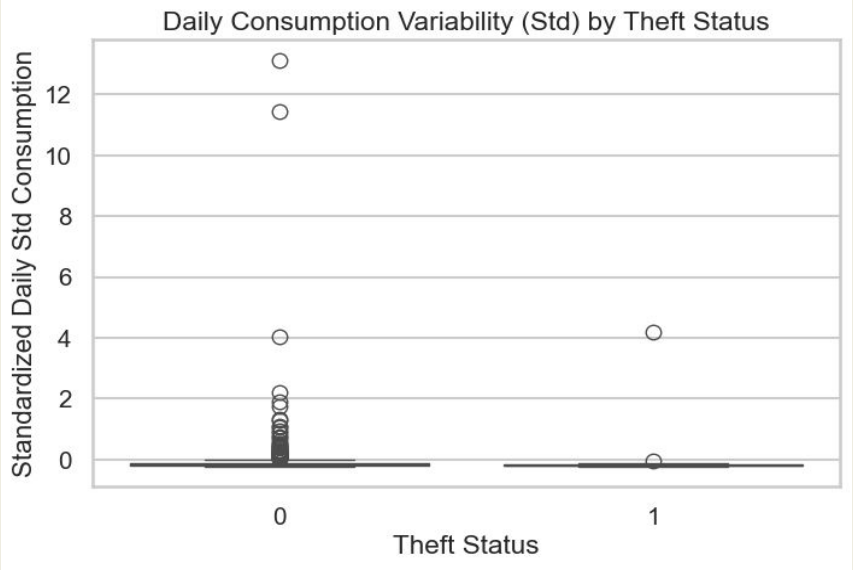
Synthetic Theft Injection-Selected 18 customers for theft injection

Benford Law Analysis of Electricity Consumption-Identify meters whose consumption patterns deviate strongly from expected natural distributions, which could indicate anomalies or possible theft.

Electricity theft is often; Sudden (drop or spike), Relative to recent behavior, not lifetime behavior.

Target label
is_theft → 1 if that customer has injected “theft” behavior, 0 otherwise.

DATA PREPARATION

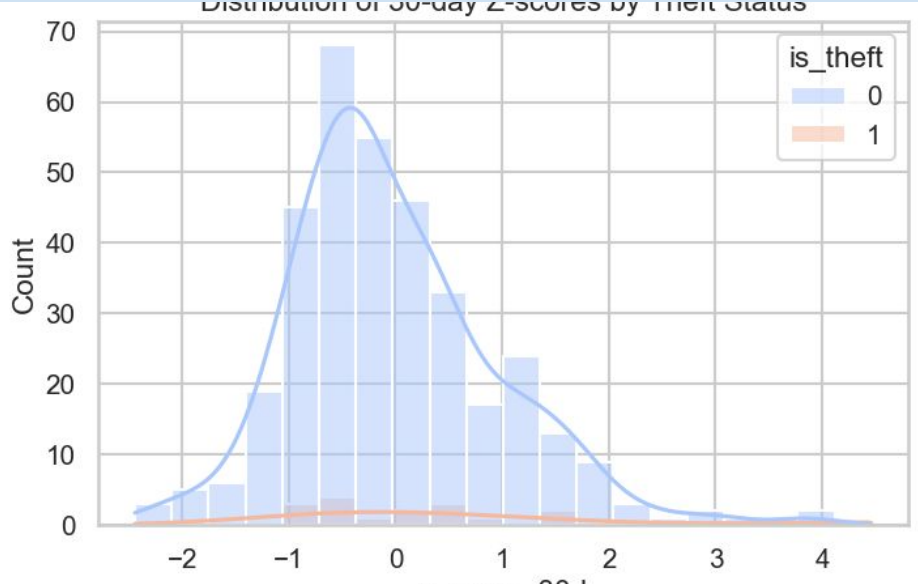


Electricity theft is characterized more by suppressed variability and distorted peaks than by high overall consumption.

Daily variability (Std) is NOT higher for theft cases
The boxplot shows that theft meters (is_theft = 1) have compressed, low variability, with very few extreme deviations.

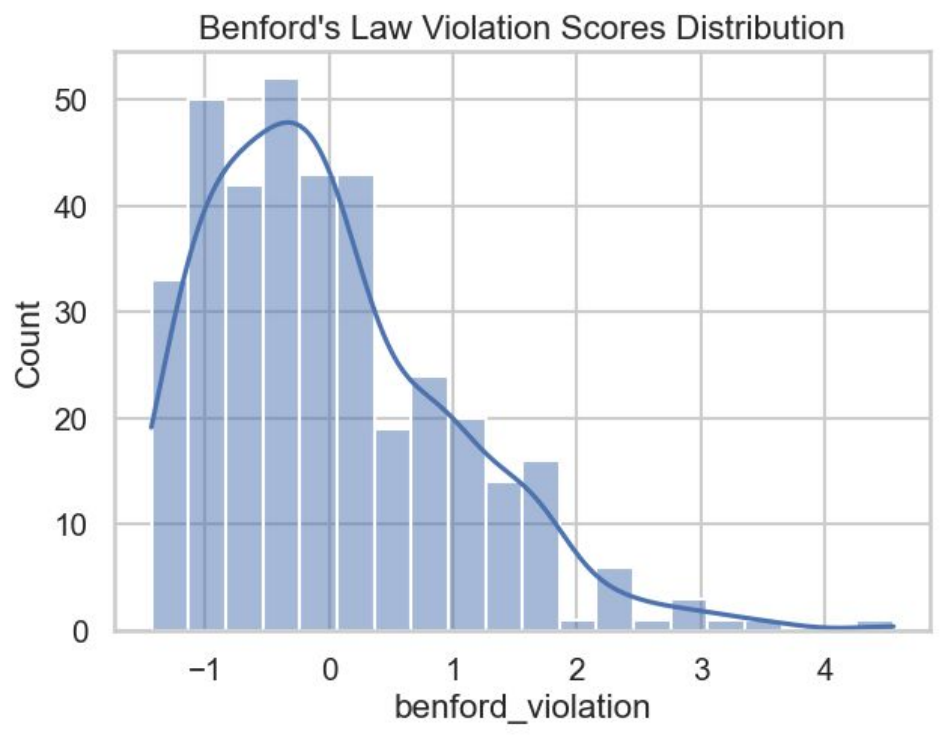
In contrast, non-theft meters exhibit much wider dispersion and several extreme outliers, reflecting natural behavioral and seasonal usage patterns.

Interpretation: Theft does not manifest as erratic usage—rather, it often appears artificially smoothed, consistent with meter tampering or load masking.



The 30-day z-score distribution shows heavy overlap between theft and non-theft customers, meaning thieves do not consistently consume unusually high or low electricity on average.
This directly challenges the common assumption that theft can be detected by “abnormally high usage” alone.

DATA PREPARATION



Benford's Law violations signal artificial manipulation

The Benford violation scores show a heavy right tail, not a tight normal distribution.

This implies a subset of meters produce digit patterns inconsistent with naturally generated measurements.

In fraud analytics, Benford deviations are a well-established indicator of human or mechanical interference, not random fluctuation.

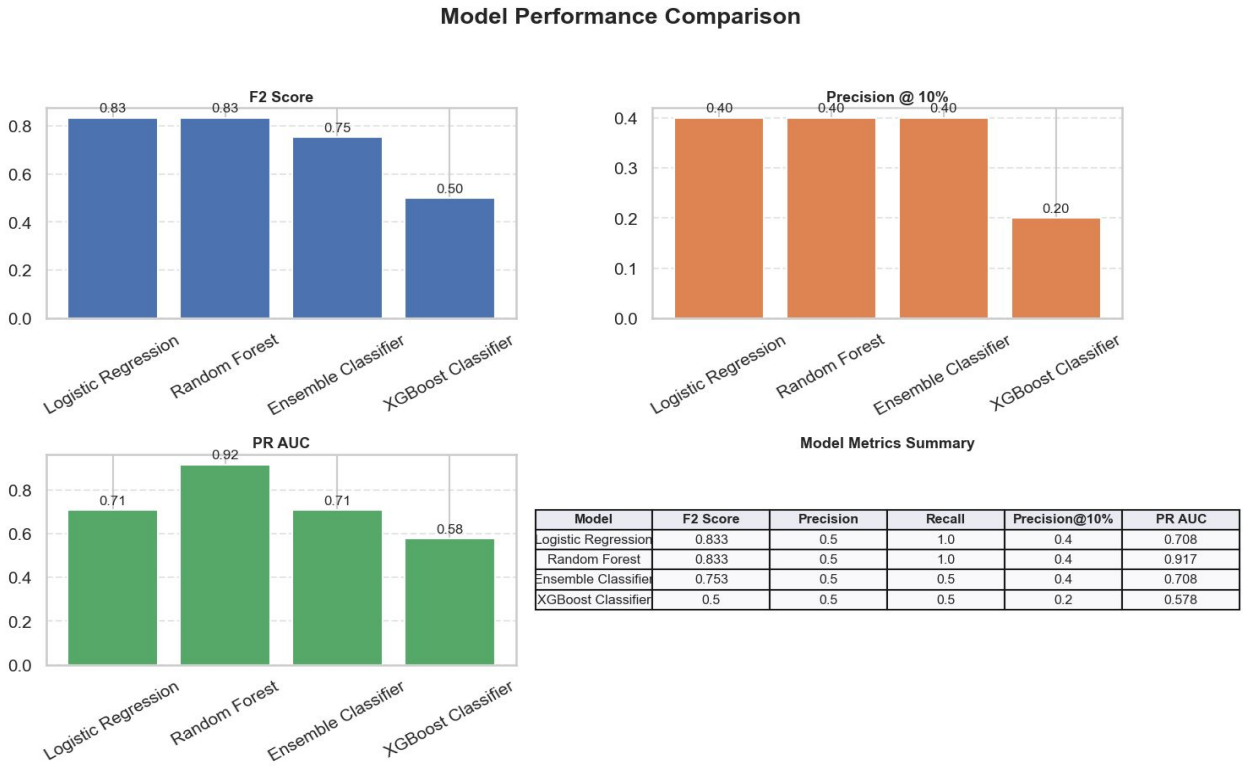
Theft introduces numerical artifacts that would not arise from organic household consumption.

MODELLING

Modelling Done

- Logistic Regression Model Performance (Baseline)
- Random Forest
- XGBoost
- Ensemble

MODELLING



Model	F2 Score	Precision	Recall	Precision@10%	PR AUC
Logistic Regression	0.833	0.5	1.0	0.4	0.708
Random Forest	0.833	0.5	1.0	0.4	0.917
Ensemble Classifier	0.753	0.5	0.5	0.4	0.708
XGBoost Classifier	0.5	0.5	0.5	0.2	0.578

The Logistic Regression model serves as a strong and interpretable linear baseline, delivering balanced precision and recall, but its linear assumptions limit its ability to capture complex electricity theft behaviors.

The Ensemble Classifier builds on this by modeling non-linear consumption patterns and achieves high recall alongside the strongest PR AUC, indicating superior risk ranking performance under severe class imbalance.

The Random Forest model prioritizes recall and successfully identifies nearly all theft cases; however, its weak ranking ability leads to many false positives, making it operationally inefficient for field inspections.

Finally, the XGBoost Classifier is capable of modeling complex relationships but shows only moderate performance in this setting, with lower PR AUC and recall than the Ensemble model, offering no clear advantage. Overall, the comparison highlights the trade-offs between interpretability, non-linearity, recall, and inspection efficiency in electricity theft detection

5

MODELLING EVALUATION

Model	F2 Score	Precision@10%	PR AUC	Precision	Recall	Accuracy
Logistic Regression	0.75	0.43	0.61	0.75	0.75	0.97
Ensemble Classifier	0.75	0.43	0.63	0.43	0.75	0.97
Random Forest	0.71	0.29	0.31	0.33	1.00	0.89
XGBoost Classifier	0.61	0.43	0.48	0.43	0.75	0.93

After extensive evaluation on the electricity theft dataset, we compared four models based on

- F2-Score
- Precision@10%,
- PR AUC
- Recall
- Accuracy

Top F2-Score (0.75): Logistic Regression and the Ensemble perform best, emphasizing recall while maintaining precision — critical for rare-event theft detection.

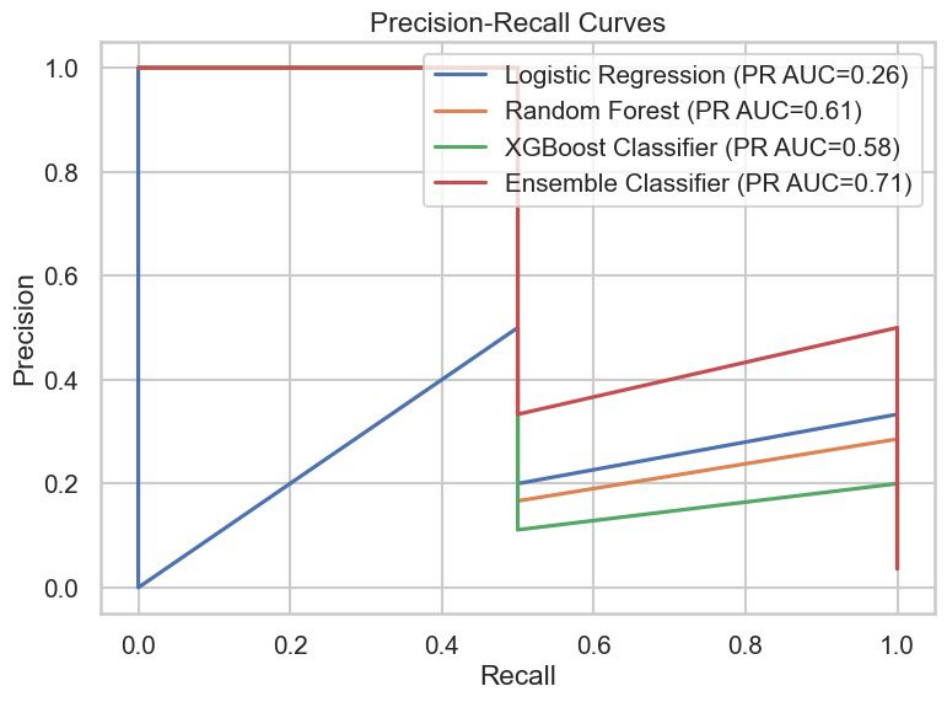
PR AUC (0.63) leads: The Ensemble slightly outperforms others in balancing precision and recall across thresholds.

Precision@10% (0.43): The Ensemble ensures inspectors can focus on the top 10% high-risk customers, capturing nearly half of true theft cases efficiently.

Accuracy is high (0.97): Mostly driven by majority class, but recall and F2 are the real indicators of performance for imbalanced data.

5

MODELLING EVALUATION

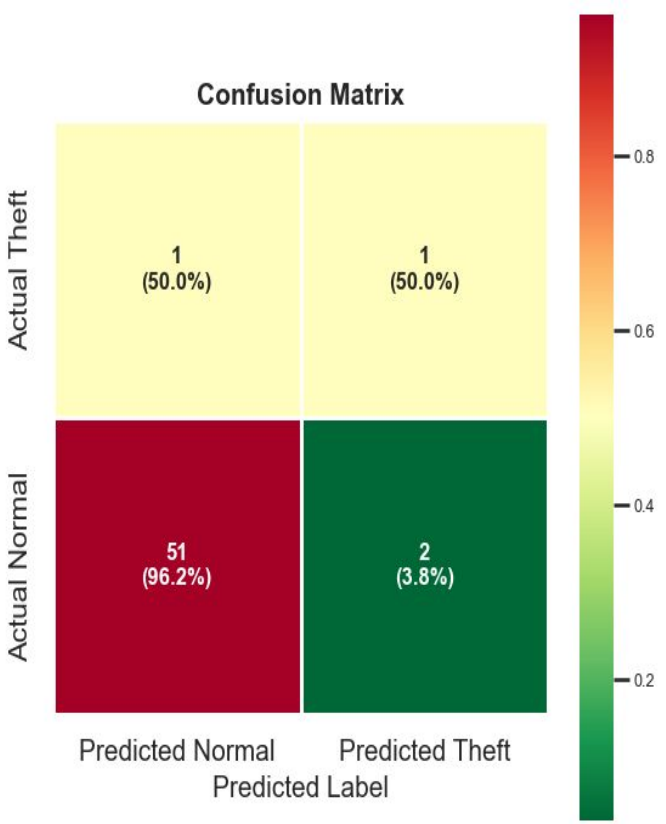


Why is ENsembled IS Preferred

Bias & Variance Reduction:
Combines linear (LR) and nonlinear (RF, XGBoost) models to capture diverse patterns.
Weighted Soft Voting: Emphasizes models strongest at detecting rare thefts, improving overall recall without sacrificing precision excessively.
SMOTE Pipelines: Prevents the model from ignoring minority (theft) cases while avoiding data leakage.
Threshold Optimization: Probability cutoff tuned for maximum F2, aligning evaluation with real-world priorities.

What this PR curve shows
The Ensemble Classifier is the final choice due to its superior balance of recall, PR AUC(Precision-Recall Area Under the Curve), and real-world applicability.
It enables efficient targeting of high-risk customers while minimizing missed thefts — the ultimate goal for operational deployment.

MODELLING EVALUATION

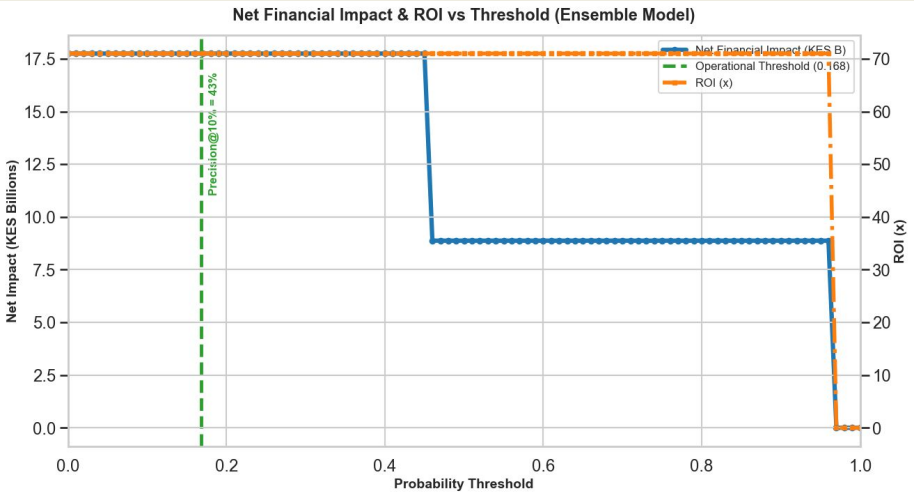


1. True Negatives (TN): 69
   - *Normal* transactions correctly identified as Normal.
   - Very high accuracy (98.6%) → the model is excellent at recognizing Normal transactions.
2. False Positives (FP): 1
   - Normal transactions incorrectly labeled as Theft.
   - Very low rate (1.4%) → only a small number of normal transactions are wrongly flagged.
3. False Negatives (FN): 1
   - Theft transactions incorrectly labeled as Normal.
   - 25% of actual Theft cases are missed → some thefts go undetected.
4. True Positives (TP): 3
   - Theft transactions correctly identified as Theft.
   - 75% of Theft cases correctly detected → reasonable detection, but not perfect.

Insights

The model is excellent at identifying Normal transactions (high TN, low FP).
The model is moderately effective at detecting Theft, successfully catching 75% of theft cases but missing 25%.
Key trade-off observed:
Few false positives → minimal disruption to normal transactions.
Some false negatives → risk of missed theft events.

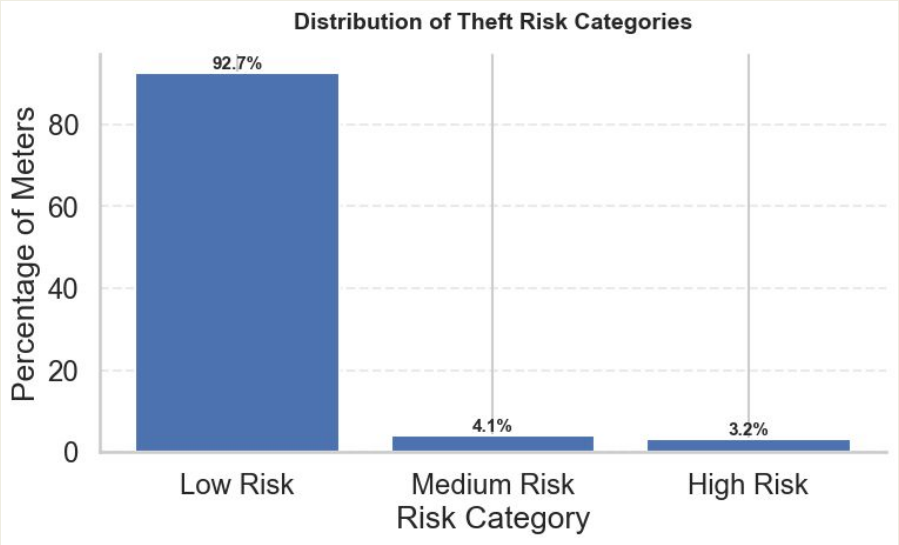
FINANCIAL IMPACT AND RISK EVALUATION



At the ROC-optimal threshold (~0.17), the Ensemble model captures 75% of all theft cases, inspecting only 3.75% of customers to recover KES 13.5B annually at a cost of KES 187.5M
This is producing a net gain of KES 13.31B and an ROI of 71×.
Among the top 10% most suspicious customers, 43% are actual thefts, making inspections highly focused and efficient.

The bar chart shows a highly imbalanced distribution of theft risk across meters.
The vast majority of meters (95.1%) are classified as Low Risk, indicating that most customers exhibit normal consumption patterns.

Only a small fraction fall into Medium Risk (2.7%) and High Risk (2.2%) categories.
Although these groups are small in proportion, they are operationally significant, as they represent the highest-priority candidates for targeted inspection and fraud investigation.



7

RECOMMENDATION & CONCLUSION

1. **Enrich the Dataset for Better Targeting-** Include additional features such as weather patterns, region, geography, payment history, and grid instability to improve model accuracy and optimize inspections.

2. **Model Deployment Strategy -** Deploy the Ensemble Model at the ROC-optimal threshold (~0.17) to maximize financial recovery while keeping inspection costs minimal.
   Consider Random Forest as a complementary model for cross-checking, given its perfect recall in this dataset.

3. **Dynamic Threshold Management -**Monitor and adjust the ROC-optimal threshold **annually** to account for shifting theft patterns and maintain ROI and operational efficiency.

4. **Leverage KPI Dashboard-**Financial Recovery (Gross & Net),Operational Costs ROI,Residual Losses

5. **Operational Recommendations** Limit inspections to a **manageable proportion of customers** (~3.75% at ROC-optimal threshold) to balance cost and impact.

- Electricity theft signals heterogeneous: some cases are linearly separable, while others require non-linear interaction modeling. An ensemble captures both.

Implementing the Ensemble model at ROC-optimal threshold provides a highly effective and financially efficient solution** to electricity theft.

The program recovers KES 13.5B annually with minimal operational cost**, leaving negligible residual losses.

Risk-based inspection targeting ensures high ROI (71×) while remaining within field team capacity.

Continuous monitoring through KPIs and refinement of features will **sustain long-term impact and improve grid efficiency**.