Smart Electricity Theft and Meter Bypass Detection

Himani Bagale[1], Harshada Bhumkar[2], Shaurya Umale[3], Pushkar Joshi[4], Abhijeet Shejwal[5], Mr. M.B. Nigade[6]

[1,2,3,4,5]*Dept. Of First Year Engineering Science, AISSMS IOIT, Pune, India*

[6]*Assistant Professor, Dept. of Mechanical Engineering, AISSMS IOIT, Pune India*

***Abstract*—Electricity theft remains a significant challenge for power distribution companies in both urban and rural areas. Traditional detection methods rely on physical inspections and manual audits. These approaches can be slow, costly, and ineffective against modern tactics like bypassing meters, illegal tapping, and changing smart meter readings. This paper presents an intelligent electricity theft detection system that uses smart metering technology, real-time monitoring, and anomaly detection methods to spot suspicious consumption patterns. The proposed system consistently compares power distribution data at the feeder level with individual consumer usage patterns to find discrepancies that may suggest unauthorized electricity use. By combining Internet of Things (IoT) sensors with machine learning techniques for spotting anomalies, the framework can identify unusual consumption trends, sudden changes in load, and meter tampering events more accurately. The system also generates alerts automatically for utility authorities, which decreases reliance on manual monitoring and allows for quicker responses. Besides improving detection, this approach aims to lower non-technical losses, increase billing transparency, and aid in creating a secure smart-grid infrastructure. The research demonstrates how combining data analysis with smart energy systems can lead to effective and scalable electricity monitoring solutions for future digital power networks.**

***Index Terms*—Electricity Theft, detection, machine learning, Internet of Things (IoT)**

I. INTRODUCTION:

Growing urbanization, industrial expansion, and increasing energy requirements have created substantial strain on electrical distribution networks globally. Simultaneously, power theft has emerged as an ongoing issue affecting the dependability, efficiency, and economic viability of utility companies. Unauthorized power consumption results in substantial revenue losses for distribution utilities while causing power imbalances, voltage fluctuations, equipment stress, and degraded service quality for authorized consumers. Power theft manifests in various forms, including direct line connections, unauthorized hookups, meter circumvention, neutral wire manipulation, and meter software modification.

Conventional electromechanical meters remain highly susceptible to physical interference methods such as magnetic disruption and wire rerouting. While contemporary smart meters provide enhanced monitoring capabilities, advanced theft techniques continue evolving, rendering traditional inspection-based detection insufficient in many situations. Existing detection approaches primarily rely on scheduled manual inspections and energy assessments. These methods demand extensive labor resources, involve substantial operational expenses, and frequently fail to identify theft activities in real time. Within extensive distribution networks serving thousands of consumers, manually identifying suspicious behavior becomes progressively difficult. Consequently, researchers and utility operators are exploring intelligent and automated detection solutions leveraging smart-grid technologies.

Recent developments in Internet of Things (IoT), wireless communication, and machine learning have created new possibilities for developing efficient electricity monitoring frameworks. Smart meters and sensor networks can collect detailed consumption information from users and transmission equipment. Combined with intelligent analytical models, these systems can identify abnormal energy consumption patterns and detect potential theft activities more efficiently. This study proposes an intelligent electricity theft and meter bypass detection framework that utilizes real-time data gathering and anomaly-driven analysis to recognize irregular electricity usage

behaviors. The system concentrates on identifying discrepancies between transformer-level distribution data and individual consumer measurements while monitoring sudden usage pattern changes that may indicate bypass situations or interference attempts. By integrating smart monitoring techniques with intelligent data processing, the system seeks to enhance detection precision, minimize non-technical losses, and strengthen the security of contemporary power distribution networks. The remainder of this document will examine the system design, detection approach, implementation plan, analytical methods, and potential applications of the proposed framework within smart-grid environments.

II. LITERATURE SURVEY:

The proposed system is designed to detect electricity theft and meter bypass activities using a combination of smart metering technology. The methodology involves system design, component integration and IoT-based monitoring.

1. System Architecture

The proposed system consists of a microcontroller (ESP32), 2 current sensors (ASC712 20A), voltage sensor (ZMPT101B AC).

2. Hardware Components

The microcontroller (ESP32) acts as the main control unit which sends the current and voltage reading to the backend, current sensor measures the amount of current flowing through the electrical line and the voltage sensor monitors supply voltage conditions continuously, the power supply section provides stable operating voltage to all electronic components.

3. Software Design

1) The software continuously collects sensor readings from the connected hardware devices. The collected data is temporarily stored before further processing.
2) The processing module converts raw sensor readings into meaningful electrical parameters.
3) The system calculates energy usage, load variations, and consumption trends.
4) Anomaly detection module identifies abnormal electricity consumption behavior.
5) Suspicious activities exceeding predefined thresholds are marked as potential theft conditions.

4. Control logic

i) Standard Operation

Under typical conditions, the system continuously monitors voltage and current values from electrical lines. The controller calculates anticipated power consumption and regularly updates the monitoring database. All measurements remain within acceptable operational parameters during normal operation.

ii) Abnormal Condition Detection

The controller compares measured values against established thresholds and historical consumption data. When sudden current imbalances or unusual power reductions occur, the system initiates verification procedures. Multiple simultaneous abnormal conditions increase theft detection probability.

iii) Theft Recognition Logic

When line current stays elevated while meter-recorded consumption drops abnormally, the system considers this a potential bypass attempt. The controller validates the abnormality over a specified observation period before generating alerts, reducing false detections from temporary variations.

iv) Alert Generation

Upon confirming theft activity, the system produces alert notifications. Alert data is transmitted to the monitoring platform through the communication module.

III. OBJECTIVES:

- To develop an intelligent electricity monitoring system
- To detect electricity theft and meter bypass activities
- To reduce non-technical power losses
- To automate theft detection processes

IV. CONCLUSION:

This project developed an intelligent electricity theft and meter bypass detection system using sensors and microcontroller technology. The system successfully identified abnormal electricity usage when meter bypass conditions were simulated. Through

measurement comparison, the setup could effectively recognize potential theft scenarios.

Hardware components including current sensors, relays, and controllers functioned properly during testing phases. The software component facilitated reading monitoring and alert generation when unusual conditions were identified. The system demonstrated reliable performance across various load conditions and responded promptly during testing.

REFERENCES:

[1] C. C. B. de Oliveira, N. Kagan, A. Meffe, S. L. Caparroz, and J. L. Cavaretti, "A new method for the computation of technical losses in electrical power distribution systems," in *Proc. CIRED*, 2001.

[2] S. Amin, G. A. Schwartz, and H. Tembine, "Incentives and security in electricity distribution networks," in *Decision and Game Theory for Security*, 2012.

[3] D. Nikovski, Z. Wang, A. Esenther, H. Sun, K. Sugiura, T. Muso, and K. Tsuru, "Smart meter data analysis for power theft detection," in *Machine Learning and Data Mining in Pattern Recognition*, Lecture Notes in Computer Science, vol. 7988, 2013, pp. 379–389.

[4] Accenture, "Achieving high performance with theft analytics," Aug. 29, 2011.

[5] Z. Xiao, Y. Xiao, and D. H.-C. Du, "Non-repudiation in neighborhood area networks for smart grid," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 18–26, 2013.

[6] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, "Smart grid metering networks: A survey on security, privacy and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2886–2927, third quarter, 2019.

[7] A. Stefanov and C.-C. Liu, "Cyber–power system security in a smart grid environment," in *Proc. IEEE PES Innovative Smart Grid Technologies (ISGT)*, 2012.

[8] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Electricity theft: Overview, issues, prevention and a smart meter-based approach to control theft," *Energy Policy*, vol. 39, no. 2, pp. 1007–1015, 2011.

[9] M. Wagner, M. Kuba, and A. Oeder, "Smart grid cyber security: A German perspective," in *Proc. Int. Conf. Smart Grid Technology, Economics and Policies (SG-TEP)*, Nuremberg, Germany, 2012, pp. 1–4.