IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 4, April 2024

Detection of False Reading Attack on Smart Energy Meter

Dr. Satish Turkane[1], Kunal Popalghat[2], Tushar Turkane[3], Vaishnavi Gunjal[4]

Department of Electronics and Telecommunication Engineering

Pravara Rural Engineering College, Loni, Maharashtra, India

Abstract*: Smart net metering systems face significant challenges related to accurate electricity measurement, safety concerns, and the threat of external tampering. False- reading attacks, which manipulate recorded usage data, undermine billing accuracy and system integrity. Safety issues, including temperature variations and gas leaks, pose risks to users and the system. External tampering, such as data manipulation or physical damage, threatens security and accurate readings. To address these challenges, a comprehensive solution is proposed to improve measurement accuracy, enhance safety measures, and establish robust security protocols. The aim is to create secure and efficient smart grid net metering systems that benefit consumers, utility providers, and the energy ecosystem as a whole. The modernization of energy distribution systems through the implementation of smart grid technologies has led to the development of advanced smart net metering systems. These systems play a crucial role in monitoring and managing electricity consumption and generation. However, as these systems rely on data communication and digital technologies, they become susceptible to various cyber threats, including false reading attacks, which can have significant financial and operational consequences for both utility companies and consumers. This project aims to address the issue of false reading attacks in smart net metering systems by proposing a detection mechanism to safeguard the integrity of the data*

Keywords: Net Metering, Electricity Measurement, False- Reading Attacks, Safety Concerns, External Tampering, Billing Accuracy, Energy Distribution, Security Protocols, System Integrity

I. INTRODUCTION

The evolution of the energy distribution landscape has witnessed a transformative leap with the deployment of Smart Net Metering Systems. These systems, equipped with advanced sensors and communication capabilities, mark a paradigm shift from traditional manual metering processes to real-time data collection and reporting. The advent of smart net metering has ushered in an era of enhanced efficiency and transparency in monitoring and billing electricity consumption. It provides instantaneous, granular data, enabling improved demand-side management, reduced energy waste, and more precise billing. However, this technological advancement has not been without its challenges. One prominent issue is the vulnerability to false reading attacks, which pose a threat to the integrity of these systems**.** The modern landscape of energy management and distribution is undergoing a transformative shift, driven by the growing prominence of smart grid net metering systems. These systems hold the promise of accurate electricity measurement, real-time monitoring, and enhanced security**.** .As the world becomes increasingly reliant on electricity, the importance of precise energy measurement cannot be overstated. Inaccurate measurements can lead to unfair billing, undermining trust between utility providers and consumers. Rising Concerns Over Security: In today's interconnected world, security is paramount. False-reading attacks on smart grid net metering systems are a real threat. Such attacks not only disrupt financial integrity but also damage the credibility of the entire energy distribution network Safety and Reliability: Ensuring the safety and reliability of these systems is an absolute necessity. Temperature variations can be indicative of technical issues or even potential safety hazards. Gas leaks are a safety concern, with the potential for catastrophic outcomes if left unaddressed. The Imperative for Efficiency: Efficient energy usage is critical for environmental sustainability. Smart grid net metering systems must not only measure electricity accurately but also encourage efficient consumption to reduce waste and carbon footprint. Consumer satisfaction and trust are at the heart of energy distribution. When users can rely on accurate readings, secure data management, and transparent billing, trust is built, leading to

DOI: 10.48175/568

long- lasting, positive relationships between utility companies and consumers. The primary motivation behind this project is to develop an effective and real-time detection mechanism to counteract false reading attacks in smart net metering systems. By doing so, the project seeks to bolster the integrity and security of the energy data being transmitted and utilized within the smart grid framework. Detecting and mitigating these attacks are imperative not only for the financial viability of utility companies but also for maintaining consumer confidence in the fairness and transparency of their energy consumption reporting.

II. LITERATURE REVIEW AND OBJECTIVE

A smart energy meter is proposed on survey [1] securing billing, load monitoring, and energy management applications by utilizing a combination of deep learning and ensemble learning approaches.

Various experiments were conducted in the Experiment 1 they tried various deep learning models, such as CNN, GRU, FFN, and LSTM and found that the GRU (Gated Recurrent Unit) outperformed the other models. With Experiment 2 they trained a GRU- based model, consisting of a GRU layer followed by a fully connected neural network and training on samples with different ratios of false readings. GRU used to capture correlation between fine-grained smart meter readings. Fully connected neural network used for accurate decision-making. In Experiment 3 in this they used GRU-based models to create an ensemble-based detector.[2] it showed that ensemble learning can reduce false alarms (FA) while quickly detecting false readings and also they compared the performance of the detector to existing literature, indicating faster detection with fewer false reading . Develop a Robust Energy Measurement System: Create a smart metering system that accurately measures electricity consumption, providing fair and precise billing for users.

Objectives of the system is to enhance Security Measures: Implement advanced security measures to detect and prevent false-reading attacks, ensuring the integrity of electricity consumption data. Ensure Real- Time Data Monitoring: Enable real-time monitoring of energy consumption data and transmit this information to a cloud-based dashboard for users and utility companies. Analyze and Detect Abnormal Usage Patterns: Develop algorithms and analysis techniques to detect abnormal electricity consumption patterns, facilitating early identification of issues

III. MATERIALS AND METHODS

Set up the smart energy meter in a controlled environment with known energy consumption patterns. Connect the smart energy meter to the data logger and computer for real-time data logging and analysis. Monitor the voltage and current signals from the smart energy meter using the oscilloscope to ensure proper operation.

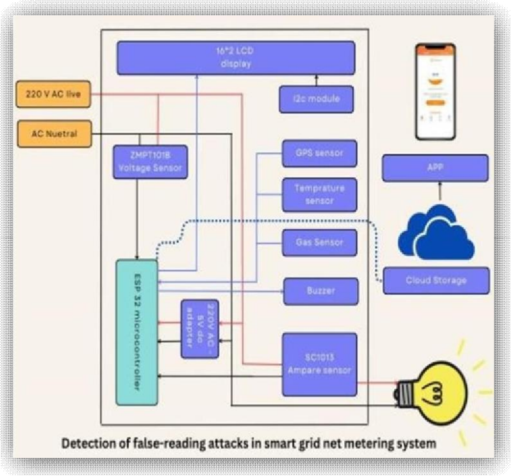

Fig 1 : Block Diagram

Create a baseline energy consumption profile for the smart energy meter under normal operating conditions. Introduce a false reading attack by manipulating the voltage or current signals to spoof higher or lower energy consumption readings. Monitor the smart energy meter readings and compare them to the baseline profile to detect any inconsistencies or anomalies. Use data analysis software to analyze the data and identify patterns indicative of a false reading attack. Implement algorithmic techniques such as anomaly detection or machine learning models to improve the accuracy of detection. Validate the detection method using known false reading attack scenarios and refine the detection algorithm accordingly.

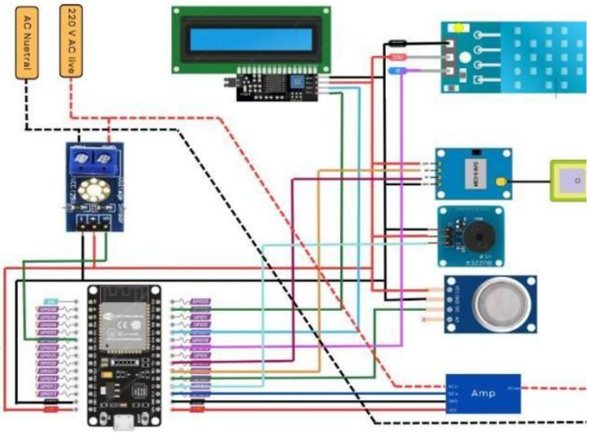

Fig 2: Circuit Diagram

- Sensor Data Acquisition: The project begins with the collection of sensor data. Current Sensors (CT) and Voltage Sensors (VT) are utilized to measure electricity consumption accurately. The data from these sensors are continuously collected and processed.
- Data Processing with ESP32: The ESP32 microcontroller plays a pivotal role in data processing. It collects, analyzes, and stores data from the sensors, ensuring real-time information about electricity usage. The ESP32 also processes location data from the GPS module.
- Enhanced Security Measures: Robust security measures are implemented to safeguard data integrity. These include encryption and authentication protocols to protect against data manipulation, as well as anomaly detection algorithms to identify unusual data patterns. Real-Time Data Transmission: Data is transmitted to a cloud-based dashboard for real-time monitoring and analysis. This enables users and utility companies to access accurate, up-to-the-minute information about electricity consumption.
- Anomaly Detection and Notification: Algorithms are employed to detect anomalies in electricity usage patterns. When significant variations or irregularities are identified, automated notifications are sent to users and utility providers, ensuring swift response to potential issues.
- Position Tracking: The GPS module actively tracks the meter's location, providing precise geospatial data. This is critical for detecting unauthorized meter movement or relocation.
- Safety Enhancement: The project utilizes sensors, including gas sensors, temperature sensors, and light sensors, to monitor safety and security. Gas sensors detect gas leaks, temperature sensors monitor temperature variations, and light sensors identify potential tampering or enclosure breaches.
- User Interface Development: A user-friendly interface with 16x2 I2C LCD displays is created to display real-time energy consumption and charges. This enhances the user experience, providing easily accessible data.

IV. CONCLUSION

The project on the “Detection of False Reading Attacks in Smart Net Metering System” has successfully addressed the critical challenges posed by malicious manipulations in energy consumption data. By deploying an integrated system comprising advanced sensors, the ESP32 microcontroller, and robust algorithms, the project ensures not only the accuracy of energy measurements but also fortifies the security of smart net metering systems. The emphasis on real-time data transmission, user-friendly interfaces, and detection algorithms contributes to a resilient and efficient energy monitoring framework.

This project holds significant promise for the future of smart grid technologies. As the energy landscape evolves, the need for precise, secure, and transparent measurement mechanisms becomes paramount. The implemented solution not only safeguards against false reading attacks but also lays the groundwork for potential integrations with emerging technologies like blockchain and advanced machine learning algorithms. The envisioned future sees this project as a cornerstone in shaping trustworthy and intelligent energy management systems.

In essence, the "Detection of False Reading Attacks in Smart Net Metering System" project not only meets its immediate objectives but also sets the stage for continued advancements in securing and optimizing energy distribution.

REFERENCES

[1]. L. J. Lepolesa, S. Achari, and L. Cheng, "Electricity theft detection in smart grids based on deep neural network," IEEE Access, vol. 10, pp. 39638–39655, 2022.

[2]. M. M. Badr, M. I. Ibrahem, M. Mahmoud, M. M. Fouda, F. Alsolami, and W. Alasmary, "Detection of false-reading attacks in smart grid net metering system," IEEE Internet of Things Journal, vol. 9, no. 2, pp. 1386–1401, 2021.

[3]. A. Takiddin, M. Ismail, M. Nabil, M. M. Mahmoud, and E. Serpedin, "Detecting electricity theft cyber- attacks in AMI networks using deep vector embeddings," IEEE Systems Journal, vol. 15, no. 3, pp. 4189–4198, 2020.

[4]. A.T.ElToukhy1,M.M.Badr,M.Mahmoud,G.Srivasta va, M.M. Fouda M.Alsabaan, "Electricity Theft Detection Using Deep Reinforcement Learning in Smart Power Grids"

[5]. M. I. Ibrahem, M. Nabil, M. M. Fouda, M. M. Mahmoud, W. Alasmary, and F. Alsolami, "Efficient privacy-preserving electricity theft detection with dynamic billing and load monitoring for AMI networks," IEEE Internet of things journal, vol. 8, no. 2, pp. 1243–1258, 2020

AUTHORS

- Kunal popalghat, BE Electronics & Telecommunication, Pravara Rural Engineering College, kunalpopalghat95@gmail.com
- Tushar Turkane, BE Electronics & Telecommunication, Pravara Rural Engineering College, t.s.turkane@gmail.com
- Vaishnavi Gunjal, BE Electronics & Telecommunication, Pravara Rural Engineering College, vaishnavigunjal96@gmail.com