GridShield: Secure Smart Meter Communication And Intelligent Energy Theft Detection System

Mrs. P. Uma Maheshwari[1], Swetha S[2], Riyashika R[3], Dhanupriya RD[4]
[1, 2, 3, 4] Dept of Computer Science and Business Systems
[1, 2, 3, 4] K. Ramakrishnan College of Engineering, Trichy, India

Abstract- *Electricity theft is one of the major challenges faced by power distribution systems, especially in developing countries like India. Traditional electricity monitoring systems mainly depend on manual inspection and basic monitoring techniques, which are inefficient in identifying real-time power theft and cyber-attacks. Smart meters are widely used for monitoring electricity consumption, but the communication between smart meters and electricity providers is vulnerable to data tampering and unauthorized access. This paper proposes GridShield, a secure smart meter communication and intelligent energy theft detection system using encryption and machine learning techniques. The proposed system encrypts smart meter data using AES encryption before transmitting it to the server, thereby ensuring secure communication. Machine learning algorithms are used to analyse electricity consumption patterns and identify abnormal usage behaviour that may indicate electricity theft. The system provides real-time alerts to electricity authorities when suspicious activity is detected. The proposed solution improves smart grid security, reduces power loss, minimizes manual monitoring, and increases theft detection accuracy. The system is scalable and suitable for smart city and smart grid environments.*

Keywords: Smart Meter, Electricity Theft Detection, Machine Learning, AES Encryption, Smart Grid Security

I. INTRODUCTION

1.1 Background

Electricity theft is one of the major problems faced by electricity distribution systems worldwide. Illegal meter tampering, meter bypassing, and false data manipulation result in huge financial losses for electricity boards. Traditional electricity monitoring systems mainly depend on manual inspection and periodic verification, which are inefficient and time-consuming.

With the development of smart grid technology, smart meters are increasingly used for monitoring electricity consumption. However, smart meter communication systems are vulnerable to cyber-attacks and false data injection attacks. Therefore, there is a need for a secure and intelligent electricity monitoring system.

1.2 Need for Smart Theft Detection

Existing electricity monitoring systems lack real-time theft detection and secure communication mechanisms. Manual monitoring methods increase operational cost and delay theft identification.

Machine learning techniques can analyze electricity consumption patterns and detect abnormal usage behavior automatically. Encryption techniques can secure smart meter communication and prevent unauthorized data manipulation.

The integration of machine learning and cybersecurity can improve smart grid reliability and reduce power losses.

1.3 Scope of the System

The proposed GridShield system can be implemented in smart cities, residential areas, industries, and commercial power distribution systems.

The system supports secure smart meter communication, intelligent theft detection, real-time alerts, and electricity usage monitoring through a web dashboard.

II. PROBLEM STATEMENT

Traditional electricity distribution systems face several challenges due to electricity theft and insecure smart meter communication. Illegal meter bypassing and fake data transmission reduce electricity board revenue and affect power distribution efficiency.

Existing systems mainly depend on manual inspection and basic monitoring techniques, which fail to detect theft in real time. Smart meters are also vulnerable to cyber attacks and data tampering.

Therefore, there is a need for an intelligent and secure system that can automatically detect electricity theft and provide secure communication between smart meters and electricity providers.

III. OBJECTIVES

3.1 Main Objective

The main objective of this project is to develop a secure smart meter communication and intelligent electricity theft detection system using machine learning and encryption techniques.

3.2 Specific Objectives

- To secure smart meter communication using AES encryption
- To detect abnormal electricity usage using machine learning
- To provide real-time theft alerts
- To reduce electricity power losses
- To improve smart grid security and monitoring

IV. LITERATURE SURVEY

Several IEEE research papers have focused on electricity theft detection and smart grid security using machine learning and cybersecurity techniques.

Recent systems use anomaly detection algorithms, smart meter data analysis, and encryption mechanisms to improve electricity monitoring. Machine learning models such as KNN, LSTM, and Decision Tree algorithms are widely used for identifying abnormal electricity consumption patterns.

Cybersecurity mechanisms are also implemented to prevent false data injection attacks and unauthorized smart meter communication.

V. PROPOSED SYSTEM

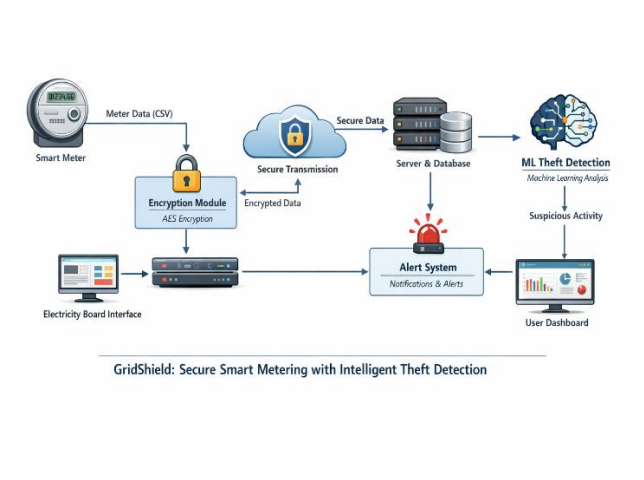
5.1 Overview

The proposed GridShield system combines machine learning and encryption techniques to provide secure smart meter communication and intelligent electricity theft detection.

The system collects electricity usage data from smart meters, encrypts the data using AES encryption, and transmits it securely to the server. Machine learning algorithms analyze the data and identify suspicious electricity consumption patterns.

5.2 Working Principle

The smart meter continuously records electricity consumption data. Before transmission, the data is encrypted to prevent unauthorized access and data tampering.



VI. SYSTEM ARCHITECTURE

The system architecture consists of multiple modules including user authentication, smart meter data upload, encryption module, machine learning analysis module, alert system, and reporting system.

The frontend interface allows users to monitor electricity consumption and suspicious activities through a dashboard. The backend server processes data securely and performs theft detection analysis.

VII. METHODOLOGY

The proposed system follows a modular development methodology for secure electricity monitoring and theft detection.Initially, smart meter data is collected and stored in the system database. The collected data includes electricity consumption, voltage, current, and timestamp information.

The encryption module secures the smart meter data using AES encryption before transmission. The encrypted data is then transmitted securely to the server.Machine learning algorithms analyse electricity consumption patterns and identify abnormal behaviour. If suspicious activity is detected, the system generates alerts and updates the dashboard.The frontend and backend modules are developed independently to improve scalability and maintainability.

VIII. HARDWARE IMPLEMENTATION

The proposed system does not require physical smart meter hardware for implementation. Simulated smart meter data is used for testing and demonstration purposes.

The hardware requirements for the system include:

- Computer or Laptop
- Internet Connectivity
- Server System
- Storage Device

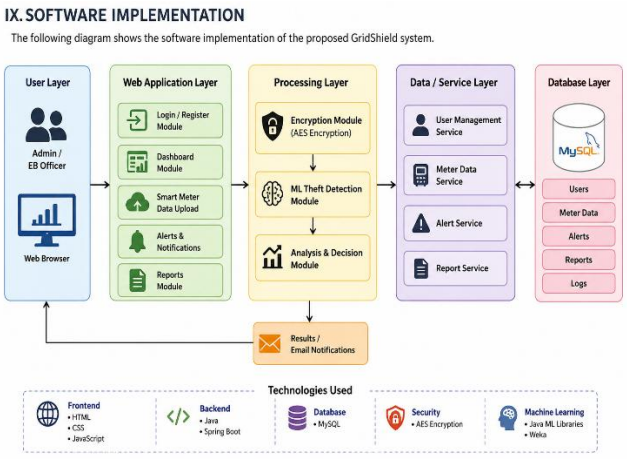
The system can later be integrated with real smart meters and IoT devices for practical deployment in smart grid environments.

IX. SOFTWARE IMPLEMENTATION

The software implementation is developed using Java and Spring Boot technologies. The frontend interface is developed using HTML, CSS, and JavaScript for creating interactive web pages and dashboards.The backend server is implemented using Spring Boot framework for secure data processing and user authentication.

MySQL database is used for storing user information, smart meter data, and alert reports.Machine learning algorithms are implemented using Java-based libraries for electricity theft detection and anomaly analysis.

AES encryption techniques are used to secure smart meter communication and prevent data tampering



X. RESULTS AND DISCUSSION

The proposed GridShield system successfully detects abnormal electricity consumption patterns and provides secure smart meter communication.The machine learning module identifies suspicious electricity usage such as sudden spikes, unusual consumption behaviour, and meter bypass patterns.The encryption module prevents unauthorized access and secures communication between smart meters and the server.The dashboard displays electricity usage statistics, alerts, and graphical analysis for efficient monitoring.The system improves electricity theft detection accuracy and reduces manual monitoring efforts.

XI. ADVANTAGES

The proposed system provides several advantages for smart grid electricity monitoring and security.

- Secure smart meter communication using AES encryption
- Intelligent electricity theft detection using machine learning
- Real-time monitoring and alert generation
- Reduced power losses and operational cost
- Improved smart grid security
- Easy monitoring through web dashboard
- Scalable for smart city applications

XII. APPLICATIONS

The proposed GridShield system can be used in various electricity distribution and smart grid environments.

- Smart Citiess
- Residential Electricity Monitoring
- Industrial Power Distribution
- Commercial Electricity Management
- Smart Grid Infrastructure
- Energy Monitoring Systems
- Electricity Board Monitoring Systems

XIII. FUTURE ENHANCEMENTS

The proposed system can be further improved by integrating advanced deep learning algorithms for higher theft detection accuracy.Real-time IoT smart meter integration can be implemented for live electricity monitoring and data collection.Cloud computing technologies can be used for large-scale smart grid deployment and remote monitoring.

Blockchain technology can also be integrated to improve data security and transparency in smart meter communication.Mobile application support can be added for real-time alert notifications and remote monitoring.

XIV. CONCLUSION

The proposed GridShield system provides a secure and intelligent solution for electricity theft detection in smart grids.The integration of machine learning and AES encryption improves electricity monitoring, smart meter communication security, and theft detection accuracy.The system successfully identifies abnormal electricity usage patterns and generates alerts for suspicious activities.The proposed solution reduces electricity theft, minimizes financial losses, and improves the efficiency of smart grid systems.The system is scalable, cost-effective, and suitable for smart city and smart grid applications.

REFERENCES

[1] N. F. Expósito et al., "Electricity theft detection in smart grids using machine learning," IEEE Access, 2021.
[2] Z. Zheng et al., "Wide and deep convolutional neural networks for electricity-theft detection," IEEE Trans. Industrial Informatics, 2018.
[3] M. Saeed et al., "Electricity theft detection in AMI using deep learning," IEEE Trans. Smart Grid, 2020.
[4] F. Jokar et al., "Electricity theft detection in AMI using customers consumption patterns," IEEE Trans. Smart Grid, 2016.
[5] R. Jiang et al., "Energy theft detection using gradient boosting theft detector," IEEE Trans. Smart Grid, 2019.