International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Electricity Theft Risk Assessment and Mitigation Using Smart Meter, IoT, AI, AMI and Automatic Power Disconnection

K.S. Gowthaman[1], V. Gurukarthikeyan[2]

Submitted: 03/01/2023 **Revised**: 18/02/2023 **Accepted**: 25/02/2023

ABSTRACT: Electricity theft is a significant issue that causes financial losses to electricity distribution authorities and affects the efficiency of energy management systems. Conventional energy meters have limited capability to identify unauthorized power consumption, meter tampering and illegal connections in real time. This paper proposes an advanced Electricity Theft Risk Assessment and Mitigation System using Smart Meter, Internet of Things (IoT), Artificial Intelligence (AI), Advanced Metering Infrastructure (AMI) and Automatic Power Disconnection. The smart meter continuously measures electrical parameters such as voltage, current, power and energy consumption. These measurements are transmitted through IoT communication modules to a centralized AMI platform for monitoring and analysis. AI-based algorithms process real-time and historical consumption data to detect abnormal usage patterns and identify potential theft activities with improved accuracy. The system assesses theft risk by comparing consumer-side measurements with authorized energy consumption records. Upon confirmation of suspicious activity, an automatic power disconnection mechanism isolates the connection to prevent further energy loss. The proposed system enables real-time monitoring, intelligent theft detection, rapid response, enhanced security and effective revenue protection. The integration of Smart Meter, IoT, AI, AMI and Automatic Power Disconnection provides a reliable and scalable solution for electricity theft prevention and efficient energy management.

KEYWORDS: *Electricity Theft Detection, Smart Meter, Internet of Things (IoT), Artificial Intelligence (AI), Advanced Metering Infrastructure (AMI), Automatic Power Disconnection, Energy Monitoring, Risk Assessment.*

1.INTRODUCTION

Electricity is one of the most essential resources for residential, commercial and industrial applications. The increasing demand for electrical energy has led to the expansion of power distribution networks and the adoption of advanced metering technologies. However, electricity theft remains a major challenge for power utilities worldwide. Unauthorized consumption of electricity through illegal connections, meter tampering, bypassing of energy meters and manipulation of meter readings results in substantial financial losses and operational inefficiencies. These activities not only reduce the revenue of electricity providers but also affect the quality, reliability and availability of power supply to legitimate consumers.

Traditional energy meters primarily record energy consumption and offer limited capabilities for detecting theft in real time. Manual inspection methods are labor-intensive, time-consuming and often ineffective in identifying sophisticated theft techniques. As electricity theft methods become more advanced, there is a growing need for intelligent monitoring systems capable of continuously analyzing energy usage patterns and detecting suspicious activities automatically.

Recent advancements in Smart Metering, Internet of Things (IoT), Artificial Intelligence (AI) and Advanced Metering Infrastructure (AMI) have created new opportunities for improving electricity theft detection and prevention. Smart meters provide detailed measurements of electrical parameters such as voltage, current, power and energy consumption. These meters can communicate with centralized

[1]*Assistant Professor, Department of Electrical and Electronics Engineering, Government College of Engineering, Thanjavur, India. Email: ksgowthaman1989@gmail.com*

[2]*Assistant Professor, Department of Mechanical Engineering, Government College of Engineering, Thanjavur, India. Email: gurumech37@gmail.com*

monitoring systems through IoT-enabled communication networks, enabling continuous data collection and remote monitoring. The collected data can then be analyzed using AI-based algorithms to identify abnormal consumption patterns that may indicate electricity theft.

Artificial Intelligence plays a crucial role in modern theft detection systems by processing large volumes of real-time and historical consumption data. Machine learning algorithms can distinguish between normal and abnormal energy usage behaviors, thereby improving the accuracy of theft detection while reducing false alarms. AI-based analysis enables utilities to assess the risk level associated with each consumer and prioritize investigations accordingly. This intelligent approach significantly enhances the efficiency of electricity theft monitoring and mitigation.

Advanced Metering Infrastructure (AMI) serves as the communication backbone of the proposed system. AMI facilitates two-way communication between smart meters and the central monitoring station, allowing utilities to collect meter data, monitor consumer energy usage and manage electrical services remotely. The integration of AMI with smart meters ensures secure and reliable transmission of energy consumption information, enabling real-time detection of anomalies and unauthorized activities.

In addition to theft detection, rapid response is essential to minimize energy losses. Therefore, the proposed system incorporates an Automatic Power Disconnection mechanism. When the system identifies and confirms a theft incident through AI-based analysis, a control signal is generated to disconnect the electrical supply to the suspicious connection automatically. This immediate action prevents further unauthorized energy consumption and enhances the effectiveness of theft mitigation efforts. Once the issue is resolved and verified by authorized personnel, the power supply can be restored safely.

The proposed Electricity Theft Risk Assessment and Mitigation System using Smart Meter, IoT, AI, AMI and Automatic Power Disconnection provides a comprehensive solution for real-time monitoring, intelligent theft detection, risk assessment and automated response. The integration of these technologies enables accurate identification of electricity theft while reducing manual intervention and operational costs. Furthermore, the system improves energy management, enhances consumer accountability and supports the modernization of electricity distribution systems.

This work aims to develop an efficient and reliable framework for detecting electricity theft, assessing associated risks and implementing appropriate mitigation measures. By leveraging the capabilities of Smart Metering, IoT communication, AI-based analytics, AMI infrastructure and Automatic Power Disconnection, the proposed system offers an advanced approach to protecting energy resources and minimizing revenue losses caused by unauthorized electricity consumption.

2.LITERATURE SURVEY

Electricity theft has become a critical issue for power utilities across the world due to the significant financial losses and operational challenges it creates. Unauthorized energy consumption through illegal connections, meter tampering, power tapping and manipulation of meter readings reduces utility revenue and affects power quality. To overcome these challenges, researchers have developed various detection and prevention techniques ranging from hardware-based monitoring systems to advanced Artificial Intelligence (AI) and Internet of Things (IoT) solutions.

Early research focused on identifying electricity theft within Advanced Metering Infrastructure (AMI) environments. McLaughlin et al. [2] investigated energy theft vulnerabilities in AMI systems and demonstrated how unauthorized users could manipulate meter communications to evade billing. Depuru et al. [3] provided a comprehensive review of electricity theft methods, causes, economic impacts and prevention techniques. Their work highlighted the importance of integrating advanced metering technologies into modern distribution networks. Jiang et al. [4] further examined theft detection challenges in AMI systems and proposed approaches for identifying discrepancies between recorded and actual energy consumption.

Several researchers proposed hardware-based solutions to detect electricity theft directly at the consumer end. Mohammad et al. [5] developed a smart prepaid energy metering system integrated with GSM communication to minimize electricity theft and improve revenue collection. Nizar et al. [6]

applied intelligent computational techniques to identify non-technical losses resulting from unauthorized electricity consumption. Jokar et al. [7] introduced a customer consumption pattern analysis method that compared expected and actual electricity usage to detect suspicious activities. These studies demonstrated that continuous monitoring of consumer energy behavior could significantly improve theft detection accuracy.

The development of Smart Meter technology created new opportunities for real-time electricity monitoring and theft prevention. Gowthaman and Gurukarthikeyan [1] proposed a Smart Anti-Theft System capable of detecting meter tampering and power tapping using sensor-based monitoring techniques. The system continuously monitored electrical parameters and generated alerts whenever unauthorized activities were detected. Faisal et al. [8] developed an IoT-enabled energy monitoring system that transmitted real-time energy consumption data to utility operators. Their work demonstrated the effectiveness of wireless communication technologies in supporting theft detection applications.

Artificial Intelligence and Machine Learning have increasingly been employed to improve the effectiveness of electricity theft detection systems. Glauner et al. [9] investigated the application of AI techniques for identifying non-technical losses and highlighted the challenges associated with class imbalance and data quality. Buzau et al. [10] utilized machine learning algorithms to classify consumers based on their energy consumption behavior and successfully detected fraudulent electricity usage patterns. Zheng et al. [11] provided an overview of smart meter technologies and emphasized their role in enabling data-driven theft detection mechanisms. Ghosh and Das [12] applied Artificial Neural Networks to distinguish between normal and abnormal electricity consumption profiles, achieving improved classification performance.

The increasing availability of smart meter data encouraged researchers to develop advanced data analytics approaches. Xiao et al. [13] proposed machine learning models capable of identifying electricity theft from smart meter readings with high accuracy. Mahmood et al. [14] reviewed wireless communication technologies suitable for smart energy systems and highlighted their significance in enabling real-time monitoring. Hasan et al. [15] demonstrated how Advanced Metering Infrastructure supports continuous collection and analysis of consumer energy data. Amin et al. [16] developed a smart meter-based monitoring system capable of detecting abnormal power consumption and alerting utility personnel.

Deep learning techniques have recently gained significant attention due to their ability to process large datasets and identify complex consumption patterns. Singh and Sharma [17] proposed a deep learning-based electricity theft detection framework capable of recognizing fraudulent behavior more accurately than traditional methods. Jindal et al. [18] introduced an AI-based risk assessment methodology that assigns theft probability scores to consumers based on historical consumption characteristics. Nabil et al. [19] investigated security challenges in IoT-enabled smart metering systems and proposed mechanisms to protect energy monitoring infrastructures from unauthorized access and cyber threats. Sahoo and Mohanty [20] utilized data analytics techniques to detect irregular consumption patterns associated with electricity theft.

The integration of IoT and cloud computing technologies has further enhanced electricity theft monitoring capabilities. Karthick et al. [21] developed a real-time theft detection framework that combines IoT sensors with cloud-based data processing. Their system enabled continuous monitoring and rapid identification of suspicious energy consumption. Ahmad et al. [22] proposed hybrid machine learning models that combine multiple classifiers to improve theft detection accuracy under varying operating conditions. Ullah et al. [23] utilized smart meter data analytics techniques to identify non-technical losses and classify consumers according to theft risk levels. Prakash and Kumar [24] introduced an IoT-enabled smart metering framework capable of providing real-time energy monitoring and theft detection functionalities.

Consumer behavior analysis has also been explored as an effective approach for theft detection. Roy and Bhattacharya [25] analyzed consumer load patterns and identified significant deviations that could indicate unauthorized electricity usage. Their work demonstrated that behavioral analytics can provide valuable insights for detecting hidden theft activities. Such approaches reduce the dependence on manual inspections and improve operational efficiency.

Recent research has focused on integrating Artificial Intelligence, IoT and AMI technologies into comprehensive electricity theft detection systems. Sharma et al. [26] proposed an AI-based framework capable of identifying electricity theft under varying load conditions using smart meter data. Al-Hawawreh et al. [27] developed an intelligent IoT-based energy monitoring system that continuously tracks consumer energy usage and detects suspicious activities. Khan et al. [28] introduced an Automatic Power Disconnection mechanism that isolates consumers involved in theft immediately after detection, thereby minimizing revenue losses and preventing further unauthorized energy consumption.

Machine learning techniques have continued to evolve for electricity fraud detection applications. Verma and Singh [29] compared multiple machine learning algorithms and identified the most effective models for smart meter fraud detection. Rahman and Islam [30] developed a real-time IoT-based energy monitoring platform capable of collecting and analyzing consumption data continuously. Patel and Shah [31] applied data mining techniques to identify hidden electricity theft patterns within large consumer datasets. Noor et al. [32] proposed an AMI-based theft detection framework that improves communication reliability and monitoring efficiency.

Risk assessment has become an important component of modern electricity theft management systems. Kumar and Mishra [33] developed a risk assessment model that prioritizes consumers according to the probability of theft occurrence. This approach enables utility providers to allocate resources more effectively and focus investigations on high-risk consumers. Sharma and Gupta [34] applied Artificial Intelligence techniques to reduce non-technical losses and improve energy management efficiency. Prasad et al. [35] integrated AI and IoT technologies into a unified electricity theft monitoring framework capable of providing real-time surveillance, anomaly detection and automated alert generation.

Although considerable progress has been made in electricity theft detection, many existing systems focus primarily on monitoring and identification rather than comprehensive mitigation. Hardware-based approaches are effective for tampering detection but often lack intelligent analytical capabilities. Similarly, machine learning-based methods provide accurate detection but may not offer immediate response mechanisms. Therefore, there is a need for an integrated framework that combines Smart Meter technology, IoT communication, Artificial Intelligence, Advanced Metering Infrastructure, risk assessment and Automatic Power Disconnection. The proposed Electricity Theft Risk Assessment and Mitigation System addresses this gap by providing real-time monitoring, intelligent theft detection, risk evaluation and automatic mitigation capabilities to reduce revenue losses and enhance energy security.

3.RESEARCH GAP

Despite significant advancements in electricity theft detection technologies, several limitations still exist in current approaches. Many early systems primarily focus on detecting meter tampering, illegal tapping or abnormal energy consumption through hardware-based monitoring techniques. Although these methods can identify theft events, they often lack intelligent analytical capabilities and are unable to accurately assess the severity or probability of theft occurrences. Furthermore, most hardware-based solutions depend on predefined thresholds, which may result in false alarms and reduced detection accuracy under varying load conditions.

The integration of Smart Meters and Advanced Metering Infrastructure (AMI) has improved real-time data collection and remote monitoring capabilities. However, many AMI-based systems are mainly designed for data acquisition and communication rather than comprehensive theft risk assessment and mitigation. Similarly, IoT-enabled monitoring frameworks provide continuous transmission of energy consumption data but frequently rely on manual intervention after theft detection, resulting in delayed response and continued revenue loss.

Artificial Intelligence and Machine Learning techniques have demonstrated improved accuracy in identifying fraudulent consumption patterns and non-technical losses. Nevertheless, most AI-based studies concentrate primarily on theft detection and classification without incorporating automatic corrective actions. In many cases, utility operators must manually verify theft incidents and disconnect the power supply, which increases response time and operational complexity. In addition, limited attention has been given to integrating risk assessment mechanisms that can prioritize consumers based on theft probability and support proactive decision-making.

Another significant limitation is the lack of a unified framework that combines Smart Meter technology, IoT communication, Artificial Intelligence, Advanced Metering Infrastructure, theft risk assessment, real-time alert generation and Automatic Power Disconnection. Existing systems often utilize these technologies independently, resulting in fragmented operation and reduced overall effectiveness. Moreover, many reported solutions focus only on theft identification and monitoring, while comprehensive mitigation strategies for preventing further unauthorized electricity consumption remain insufficiently addressed.

Therefore, there is a clear research gap in developing an integrated and intelligent electricity theft management system that not only detects theft accurately but also evaluates theft risk, provides real-time monitoring, generates instant alerts and automatically disconnects the power supply when unauthorized usage is confirmed. To address these limitations, the proposed "Electricity Theft Risk Assessment and Mitigation Using Smart Meter, IoT, AI, AMI and Automatic Power Disconnection" framework integrates multiple advanced technologies into a unified platform capable of performing real-time monitoring, intelligent theft detection, automated risk assessment and immediate mitigation. This approach aims to reduce non-technical losses, improve utility revenue protection, enhance grid reliability and strengthen overall energy security.

4.PROPOSED SYSTEM WITH BLOCK DIAGRAM

The proposed system provides several advantages over existing methods. It enables continuous real-time monitoring, intelligent theft detection, automated risk assessment, rapid response and remote management. The integration of Smart Meter, IoT, AI, AMI and Automatic Power Disconnection creates a unified framework capable of improving detection accuracy, reducing operational costs and enhancing the security and reliability of electricity distribution systems.

Table 1 presents a comparison between existing electricity theft detection systems and the proposed Electricity Theft Risk Assessment and Mitigation System.

Table 1. Comparison of Features between Existing Systems and the Proposed System

Ref. No	Method	Smart Meter	IoT	AI	AMI	Risk Assessment	Auto Disconnection	Major Limitation
[1]	Tamper Detection	No	Yes	No	No	No	No	Detects only physical tampering
[5]	GSM Smart Meter	Yes	Limited	No	No	No	No	No intelligent analysis
[7]	Consumption Pattern Analysis	Yes	No	Limited	Yes	No	No	Detection only

[8]	IoT Monitoring	Yes	Yes	No	No	No	No	No automated decision-making
[10]	Machine Learning Detection	Yes	No	Yes	No	No	No	Requires large datasets
[13]	ML Smart Meter Analysis	Yes	No	Yes	No	No	No	No theft mitigation
[15]	AMI Monitoring	Yes	No	No	Yes	No	No	High infrastructure cost
[18]	AI Risk Assessment	Yes	No	Yes	No	Yes	No	No automatic response
[21]	IoT + Cloud Monitoring	Yes	Yes	Limited	No	No	No	Detection only
[22]	Hybrid Machine Learning	Yes	No	Yes	No	No	No	Complex model training
[28]	Automatic Disconnection	Yes	Yes	Limited	No	No	Yes	Possible false disconnection
Proposed System	Smart Meter + IoT + AI + AMI + Risk Assessment + Automatic Disconnection	Yes	Yes	Yes	Yes	Yes	Yes	Overcomes limitations of existing systems

Table 2 illustrates how Smart Meter, IoT, AI, AMI, Risk Assessment and Automatic Power Disconnection work together to achieve efficient electricity theft detection and mitigation.

Table 2. Generalized Parameters Comparison of the Proposed Electricity Theft Risk Assessment and Mitigation System with Existing Systems

Parameters	Existing Systems	Proposed System
Monitoring Method	Periodic or manual monitoring	Continuous real-time monitoring
Meter Type	Conventional meter or basic smart meter	Advanced Smart Meter
Communication	Limited communication or GSM-based	IoT-enabled communication
Data Collection	Periodic data acquisition	Continuous real-time data collection
Theft Detection	Tampering detection only or consumption analysis only	Tampering detection and consumption anomaly detection
Intelligence Level	Rule-based or threshold-based detection	AI-based intelligent detection
Risk Assessment	Not available in most systems	Automated theft risk assessment
Data Analysis	Basic monitoring and comparison	Real-time AI-driven analytics
Response Time	Delayed response due to manual verification	Immediate detection and response
Alert Generation	Alert only	Instant alert with automatic action
Power Control	Manual disconnection required	Automatic power disconnection
Remote Monitoring	Limited support	Full remote monitoring through IoT and AMI
Theft Prevention	Detects theft after occurrence	Detects and prevents further theft
Accuracy	Moderate accuracy	High detection accuracy
Human Intervention	High	Minimal
Revenue Loss Reduction	Partial reduction	Significant reduction
Security Level	Moderate	Enhanced security
Scalability	Limited scalability	Highly scalable
Maintenance Cost	High due to manual inspections	Reduced maintenance cost
System Integration	Individual technologies used separately	Smart Meter + IoT + AI + AMI + Automatic Power Disconnection integrated

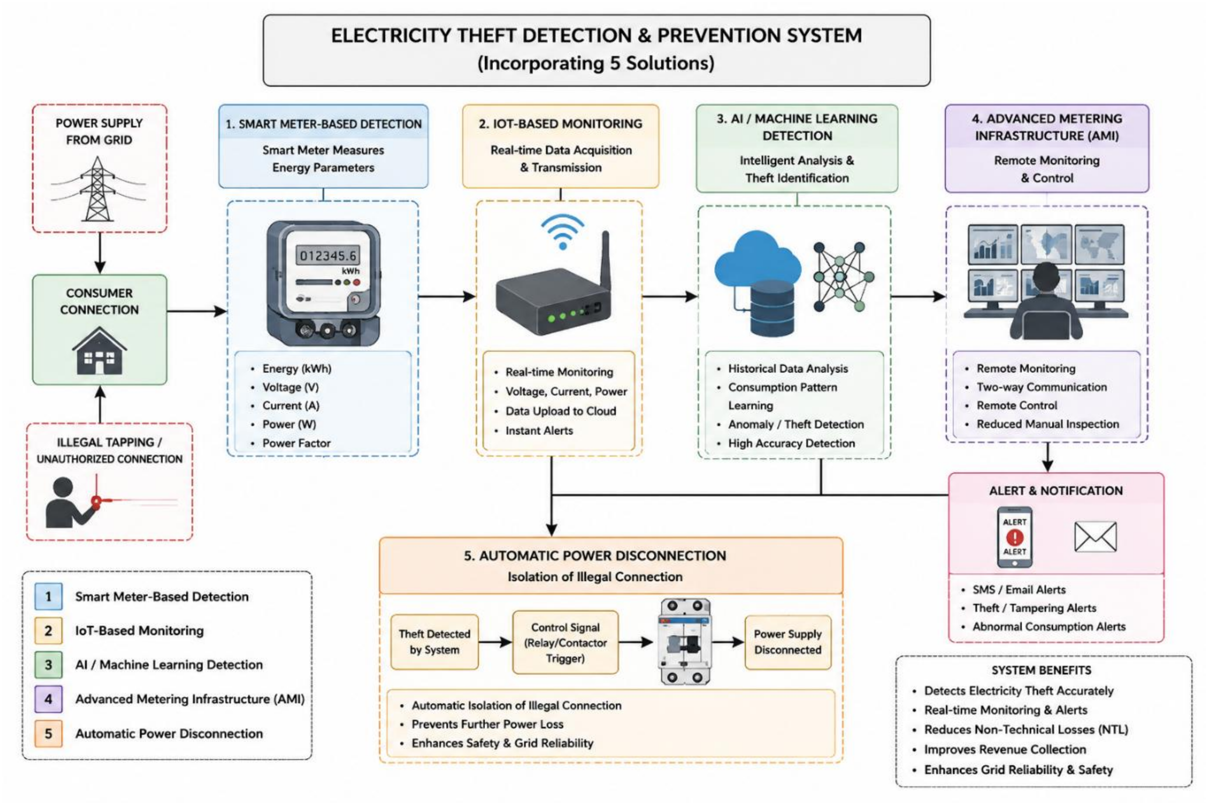

Figure 1. Proposed Electricity Theft Detection and Prevention System

Figure 1 illustrates the architecture of the proposed Electricity Theft Detection and Prevention System, which integrates Smart Meter-Based Detection, IoT-Based Monitoring, Artificial Intelligence (AI)/Machine Learning Detection, Advanced Metering Infrastructure (AMI) and Automatic Power Disconnection to identify and mitigate electricity theft in real time. The system continuously monitors energy consumption, analyzes consumer behavior, detects abnormal activities and automatically disconnects the power supply when unauthorized electricity usage is confirmed.

Initially, electrical power is supplied from the utility grid to the consumer through an authorized connection. However, electricity theft may occur through illegal tapping or unauthorized connections that bypass the energy meter. To detect such activities, a smart meter is installed at the consumer premises. The smart meter continuously measures important electrical parameters including energy consumption, voltage, current, power and power factor. These measurements provide accurate information regarding the consumer’s electricity usage and serve as the primary source of data for theft detection.

The measured data is transmitted through the IoT-based monitoring unit. The Internet of Things communication module enables real-time acquisition and transmission of electrical parameters to a centralized monitoring platform or cloud server. Through continuous communication, the utility provider can remotely access consumption data and receive instant updates regarding consumer energy usage. This real-time monitoring capability significantly improves visibility into the distribution network and enables rapid identification of suspicious activities.

The collected data is then processed by the Artificial Intelligence and Machine Learning detection module. This module analyzes both historical and real-time consumption patterns to identify abnormalities that may indicate electricity theft. Machine learning algorithms learn normal consumer behavior and compare incoming data with expected consumption characteristics. Any significant deviation, such as unusual load variations, sudden consumption changes or discrepancies between measured parameters, is classified as a potential theft event. The AI-based approach improves detection accuracy and reduces false alarms compared to conventional rule-based systems.

The Advanced Metering Infrastructure (AMI) serves as the communication and control framework of the system. AMI facilitates two-way communication between smart meters and the utility control center, enabling remote monitoring, remote data collection and system management. Utility operators can continuously observe consumer energy usage, analyze consumption trends and respond quickly to theft-related incidents without requiring physical inspections.

When the system identifies a theft event, the alert and notification module generates warning messages and sends them to utility personnel through SMS, email or monitoring dashboards. These alerts provide immediate information regarding theft attempts, abnormal consumption patterns or unauthorized connections, enabling timely decision-making and corrective action.

To prevent further energy loss, the proposed system incorporates an Automatic Power Disconnection mechanism. Once electricity theft is confirmed, a control signal is sent to a relay or contactor unit. The relay automatically disconnects the consumer from the power supply, thereby isolating the illegal connection and preventing continued unauthorized electricity consumption. This automated response reduces revenue losses and enhances the overall reliability of the distribution network.

The integrated operation of Smart Meter-Based Detection, IoT-Based Monitoring, AI Analysis, AMI Communication and Automatic Power Disconnection provides a comprehensive solution for electricity theft management. The system enables accurate theft detection, real-time monitoring, intelligent decision-making, rapid response and effective mitigation. Consequently, it improves revenue collection, reduces non-technical losses, minimizes manual inspections and enhances the security and reliability of electrical power distribution systems.

5.PROPOSED PROTOTYPE MODEL

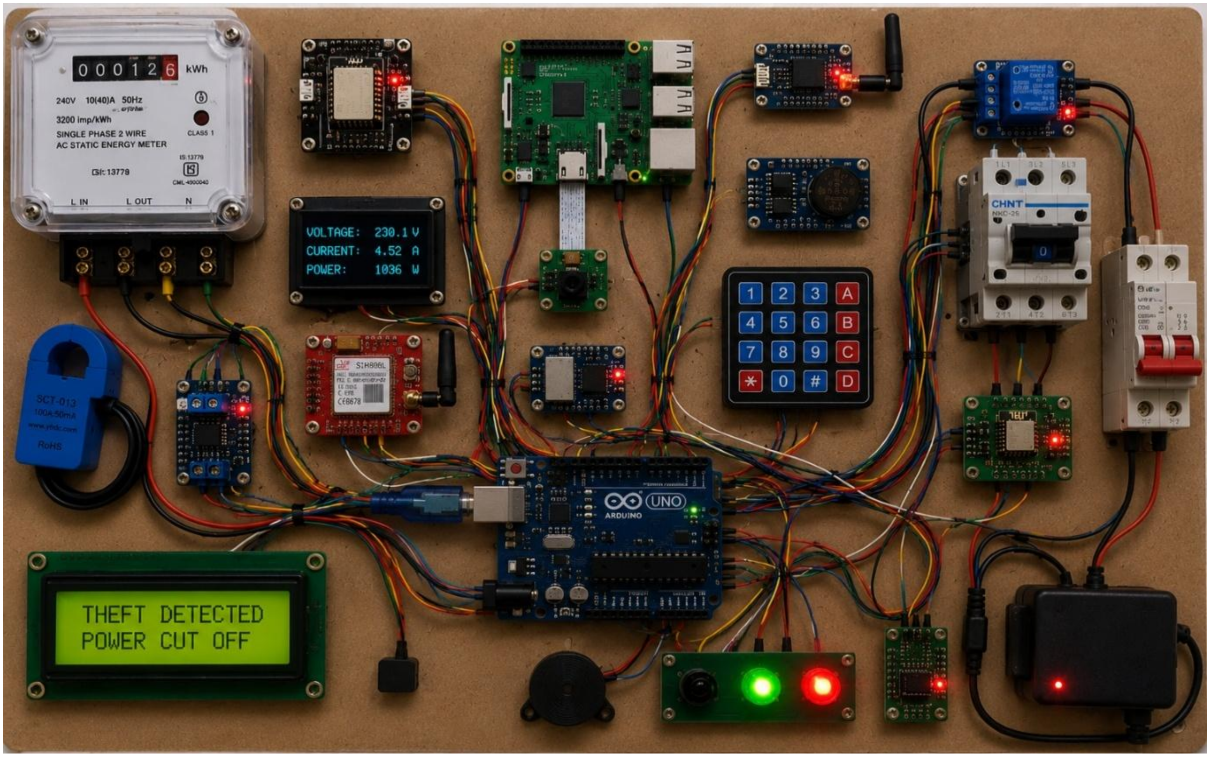

Figure 2. Hardware Prototype of the Proposed Electricity Theft Risk Assessment and Mitigation System

The proposed Electricity Theft Risk Assessment and Mitigation System in Figure 2 is designed to detect unauthorized electricity usage, assess theft risk using intelligent analysis, provide remote monitoring through IoT and AMI communication and automatically disconnect the power supply when theft is confirmed. The complete prototype is assembled on a wooden base board using commercially available electronic modules and interconnected through jumper wires. At the left side of the kit, a domestic digital energy meter is used to represent the consumer electricity meter.

This meter measures the electrical energy consumed by the load and serves as the primary source of consumption data. The meter readings are continuously monitored by the system for theft analysis.

The Arduino Uno located at the center of the kit acts as the main controller. It collects measurement data, coordinates communication among different modules, performs preliminary calculations and controls the protection mechanism. All sensing, communication and decision-making operations are synchronized through the controller. The Raspberry Pi placed at the upper-right section functions as the AI processing unit. It receives electrical data from the controller and performs intelligent analysis by comparing real-time consumption patterns with expected behavior. The AI module helps identify anomalies that may indicate electricity theft, meter tampering or unauthorized power extraction.

An IoT communication module is connected to the system to enable cloud-based monitoring. This module transmits real-time electrical parameters, system status and theft alerts to a remote monitoring platform. Utility authorities can access the data remotely and monitor consumer energy usage continuously. The AMI communication module provides communication between the consumer meter and the utility server. It supports remote meter reading, data transmission and verification of consumption records. This communication infrastructure helps validate theft events and improves the reliability of the monitoring process.

The relay module positioned below the controller acts as the automatic power disconnection unit. When the system confirms electricity theft, the controller activates the relay. The relay opens the supply circuit and isolates the load from the electrical source, preventing further unauthorized energy consumption. A 16×2 LCD display is provided to display system messages and operating conditions. During normal operation, the display indicates that the system is functioning normally. When theft is detected, the display shows warning messages such as "THEFT DETECTED" and "POWER CUT OFF." The buzzer module is used for audible alert generation. Whenever a theft event occurs, the buzzer is activated to notify nearby personnel and indicate that immediate attention is required. The LED indicator panel provides quick visual indication of system status. Under normal conditions, the communication indicator remains active while the alert indicator remains OFF. During theft conditions, the alert indicator turns ON and remains active after power disconnection, providing a clear visual warning of unauthorized electricity usage.

The push-button switches mounted on the right side of the board are used for system control functions such as initialization, testing, acknowledgment and reset operations during demonstration and experimentation. The SMPS power supply unit located at the lower-left side converts the incoming AC supply into regulated DC voltage required by the electronic modules. It supplies stable operating power to the controller, communication modules, display unit and protection circuitry.

During normal operation, electrical parameters are continuously acquired from the energy meter and processed by the controller. The data is transmitted to the IoT and AMI modules while simultaneously being analyzed by the AI module. If the measured values remain within acceptable limits, the system continues monitoring without interruption. If abnormal energy consumption or meter bypass conditions are detected, the AI module identifies the theft risk and generates an alert. The controller then activates the relay module, disconnecting the electrical supply automatically. The event is recorded, communicated to the utility authority and displayed on the LCD screen. After verification and corrective action, the system can be reset and normal power supply can be restored.

Thus, the developed kit demonstrates an integrated solution for Electricity Theft Risk Assessment and Mitigation Using Smart Meter, IoT, AI, AMI and Automatic Power Disconnection, providing improved energy security, reduced revenue loss, enhanced monitoring capability and safer power distribution.

5.1 MODES OF OPERATION

Figure 3 illustrates the operational workflow of the proposed Electricity Theft Risk Assessment and Mitigation System, which integrates Smart Meter, IoT, Artificial Intelligence (AI), Advanced Metering Infrastructure (AMI) and Automatic Power Disconnection technologies for effective electricity theft detection and prevention.

The process begins with system initialization, where all hardware and software modules perform self-check operations to ensure proper functioning before monitoring starts.

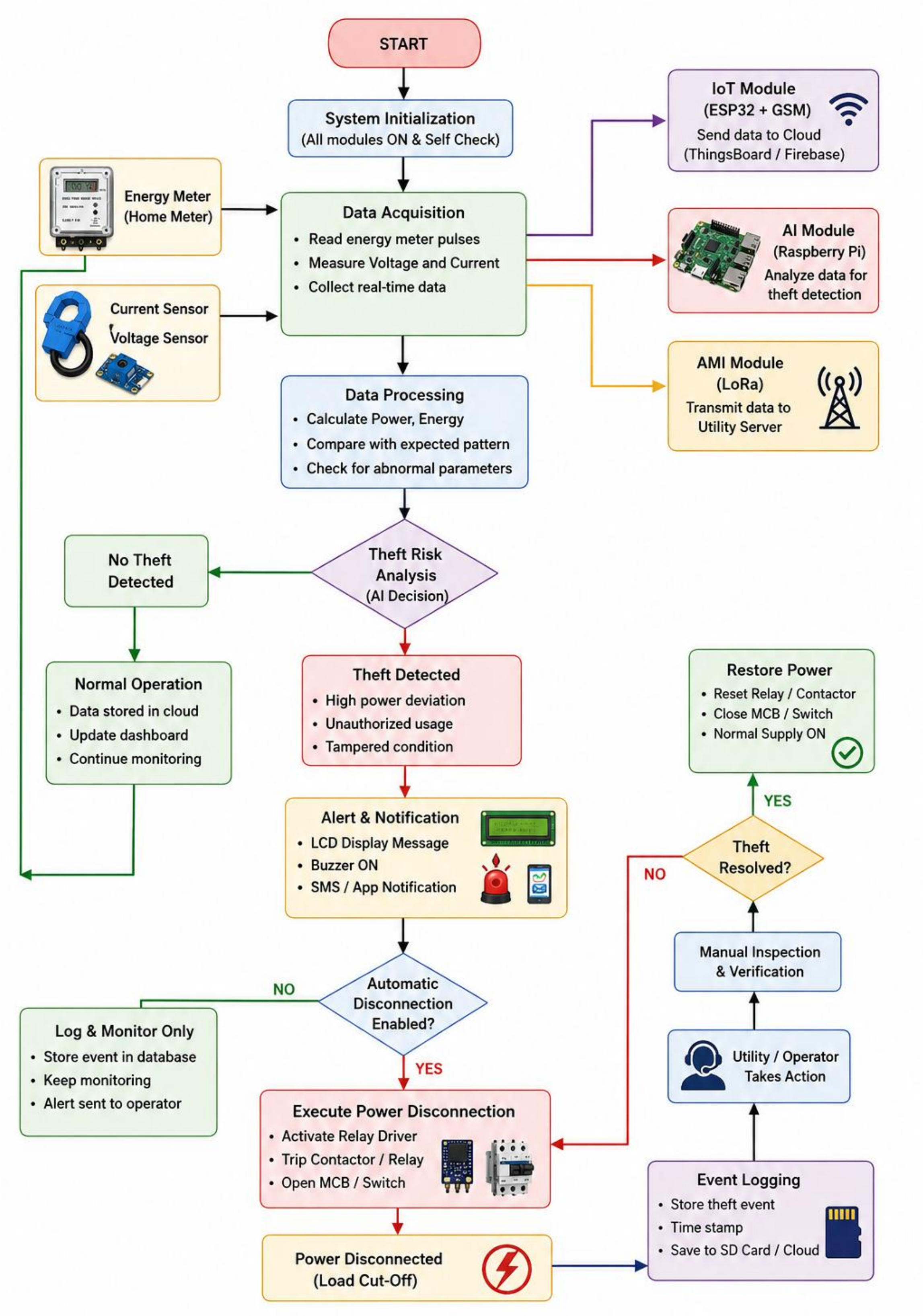

Figure 3. Flowchart of the Proposed Electricity Theft Risk Assessment and Mitigation System

5.1.1 Normal Mode Operation

When the system is powered ON, all hardware modules including the energy meter, voltage sensor, current sensor, IoT module, AI processing unit, AMI communication module, LCD display and relay control circuit are initialized and checked for proper operation. Once the self-check process is completed successfully, the system enters the normal monitoring mode. Electrical energy from the utility supply passes through the authorized energy meter and is delivered to the consumer load. The voltage and current sensors continuously measure the electrical parameters and send the collected data to the controller for processing.

During the data acquisition stage, real-time values such as voltage, current, power and energy consumption are collected and stored. The controller calculates the power usage and compares the measured values with the expected operating conditions. Simultaneously, the IoT module transmits the collected information to the cloud platform, allowing remote monitoring of consumer energy usage. The AMI communication module forwards the meter data to the utility server, ensuring that consumption information is available for remote supervision and billing purposes.

The AI module continuously analyzes the incoming data and compares it with historical consumption patterns. Since the consumer is using electricity legally, the measured energy consumption matches the expected load demand. No abnormal variations, sudden load changes, unauthorized connections or meter bypass conditions are detected. The AI algorithm therefore classifies the condition as a normal operating state.

After the theft risk analysis stage, the system follows the “No Theft Detected” path. The LCD display indicates that the system is operating normally and that no theft has been identified. The communication module continues updating the cloud dashboard with the latest consumption data. Event records are stored periodically for future reference and the monitoring process continues without interruption. Since no suspicious activity exists, the relay remains inactive, the power supply stays connected and the consumer receives uninterrupted electrical service. The entire monitoring cycle repeats continuously to ensure that any future abnormal condition can be detected immediately.

5.1.2 Theft Mode Operation

When an unauthorized electrical connection is made or an attempt is made to bypass the energy meter, the actual power consumed by the load becomes different from the energy recorded by the meter. As the system continues monitoring, the voltage and current sensors detect abnormal electrical behavior. The collected measurements are transferred to the controller, where power and energy calculations are performed. The controller identifies inconsistencies between the measured electrical parameters and the expected operating values.

The real-time data is simultaneously transmitted to the IoT platform, AMI communication network and AI processing unit. The AI module compares the incoming readings with historical consumption records and consumer usage patterns. Significant deviations such as unusual current flow, sudden load increases, abnormal energy consumption, meter tampering or unauthorized power extraction are recognized as indicators of electricity theft. Once the deviation exceeds the predefined threshold, the AI system classifies the event as a potential theft condition.

Following the theft risk analysis stage, the system enters the “Theft Detected” path. The LCD display immediately shows the message “THEFT DETECTED” and “POWER CUT OFF.” At the same time, the alert indicator is activated and a notification is generated. The IoT module sends warning messages and event information to the cloud platform, while the AMI module communicates the theft event to the utility server. All relevant details, including time, date, electrical measurements and event status, are stored in the event logging database for future investigation.

After the alert process, the controller checks whether automatic disconnection is enabled. If automatic protection is active, the controller energizes the relay driver circuit. The relay driver activates the relay or contactor, which opens the power path between the supply and the consumer load. This action immediately disconnects the electrical supply, preventing further unauthorized energy consumption. The load is isolated from the power source, thereby reducing revenue loss, preventing equipment overloading and minimizing electrical safety hazards.

Once power disconnection has been executed, the system enters the Power Disconnected state. Even though the load supply is cut off, the communication modules remain operational so that the theft event can continue to be reported to the utility authority. The event details are permanently stored in cloud storage or local memory for documentation purposes. Utility personnel can then inspect the installation and verify the cause of the theft event.

After corrective measures have been taken and the unauthorized connection has been removed, the utility operator performs a manual inspection and verification process. If the theft condition is successfully resolved, the system follows the "Theft Resolved" path. The relay or contactor is reset, the supply connection is restored and the consumer's electrical service returns to normal operation. The system then re-enters monitoring mode and resumes continuous surveillance of electrical parameters to detect any future theft attempts.

6. EXPERIMENTAL RESULTS

6.1 LCD and LED Status Monitoring Results

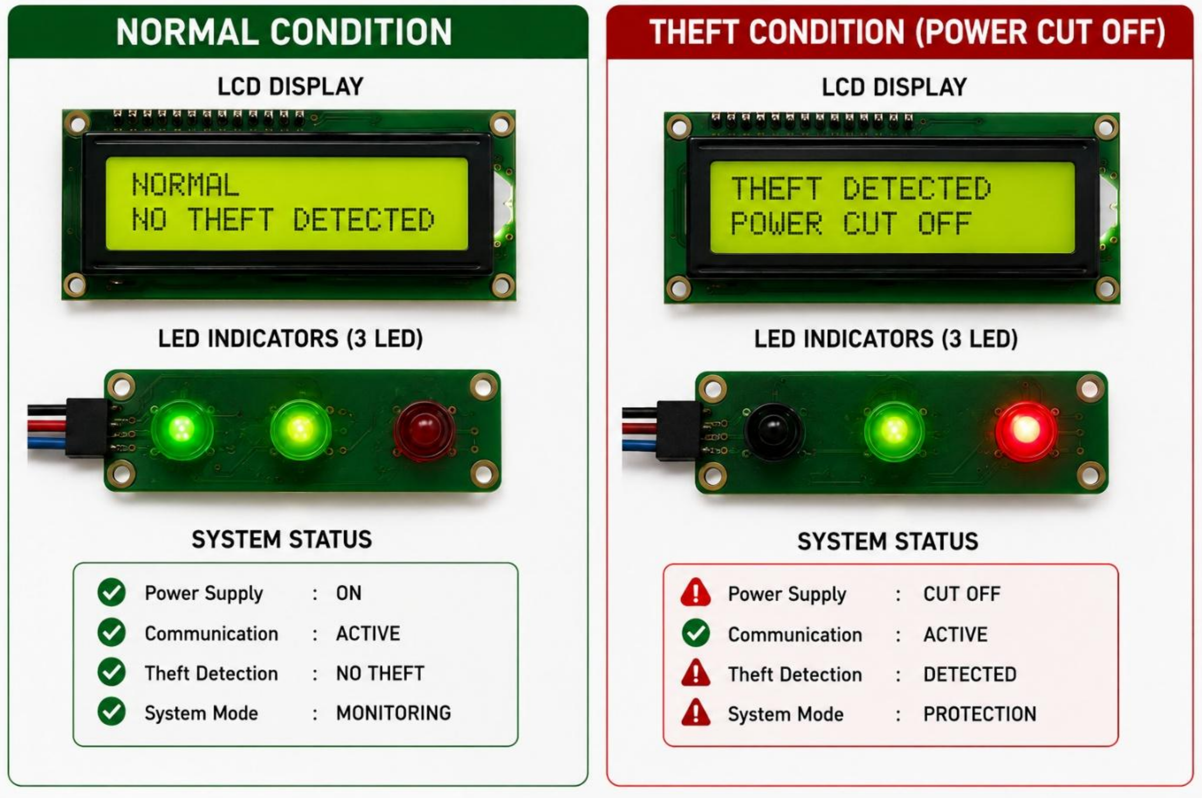

Figure 4. LCD Display and System Status Indications under Normal and Theft Conditions

The output of the proposed Electricity Theft Risk Assessment and Mitigation System in Figure 4 can be observed through the LCD display, LED indicators, buzzer alert, relay operation and communication modules. The outputs vary depending on whether the system is operating under normal conditions or theft conditions.

During normal operation, the energy consumed by the load matches the energy recorded by the meter. The controller receives the measured data from the sensing section and verifies that all electrical parameters are within the acceptable range. Since no abnormal consumption is detected, the AI module classifies the condition as normal.

The LCD display shows a normal operating message indicating that no theft has been detected. The communication indicator remains active, confirming that data is being transmitted successfully to the monitoring platform. The alert indicator remains OFF because there is no unauthorized usage. The buzzer remains silent and the relay stays in its normal state, allowing power to reach the load without interruption. Simultaneously, the IoT and AMI modules continue transmitting consumption data to the cloud and utility server for monitoring and record keeping.

When an unauthorized connection, meter bypass or abnormal power consumption pattern is detected, the AI module identifies the event as a theft condition. After verification, the controller initiates the protection sequence.

The LCD display immediately shows the messages:

THEFT DETECTED

POWER CUT OFF

The alert indicator turns ON to provide a visual warning of the theft event. The buzzer is activated to generate an audible alarm and notify nearby personnel. The IoT module sends theft notifications and system status updates to the cloud platform, while the AMI module forwards the event information to the utility server.

The controller then activates the relay module, which disconnects the electrical supply from the load. As a result, the consumer load is isolated from the power source, preventing further unauthorized energy consumption. Even after disconnection, communication modules continue operating so that event information can be transmitted and stored.

6.2 Mobile Application Monitoring and Alert Notification Results

The AMI (Advanced Metering Infrastructure) module is responsible for providing two-way communication between the electricity meter and the utility monitoring system. Whenever the system detects an abnormal condition or electricity theft, the AMI module automatically generates alert notifications and transmits the information to the concerned authorities and monitoring platforms shown in Figure 5.

In the proposed system, the AMI module sends status updates at different stages of operation. During normal operation, the AMI system periodically reports meter readings and communication status to confirm that the consumer connection is functioning properly. These messages indicate that energy consumption data is being transmitted successfully and that the monitoring network is active.

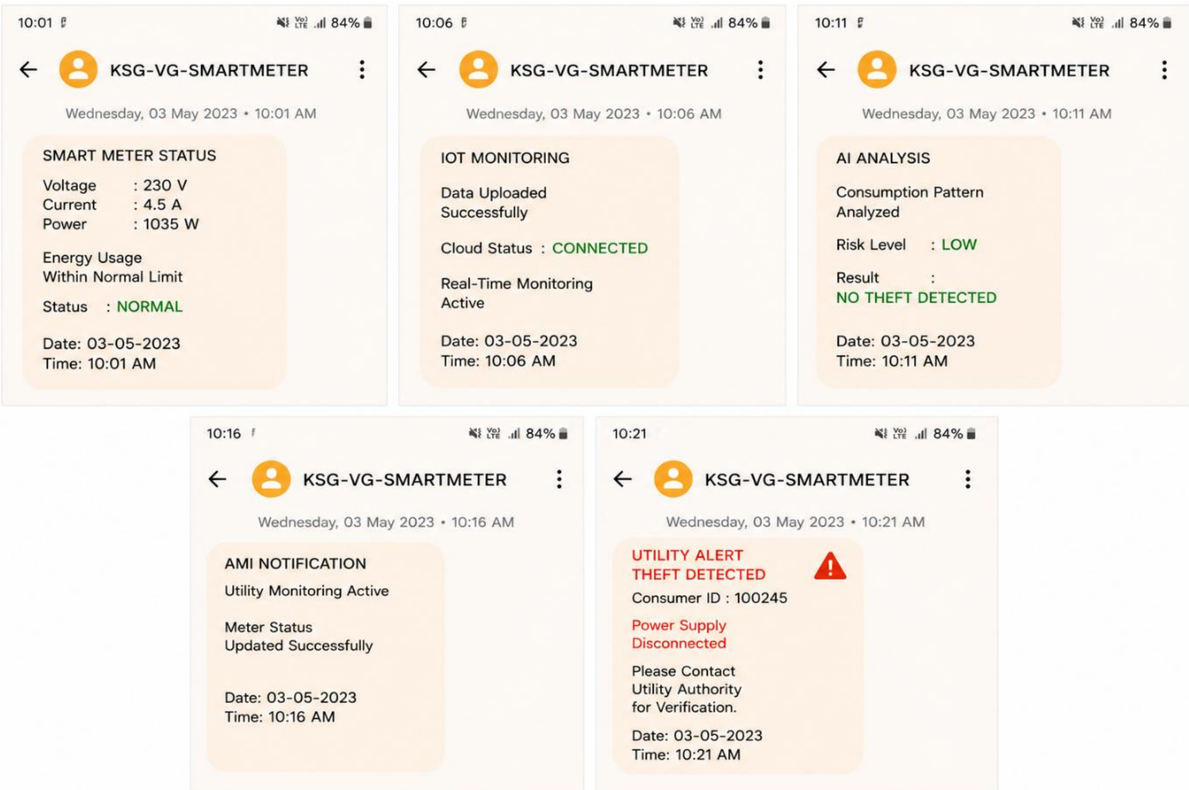

Figure 5. Mobile Dashboard Outputs of Smart Meter, IoT, AI and AMI Modules

When the AI module identifies suspicious energy usage and confirms a theft condition, the AMI module immediately generates a theft alert message. The notification contains important information regarding the detected event, including the theft status and the protective action taken by the system. This ensures that utility personnel are informed without delay and can initiate verification procedures.

After theft detection, the automatic power disconnection unit isolates the supply. The AMI module then sends another notification indicating that the power supply has been disconnected to prevent further unauthorized electricity consumption. This message acts as confirmation that the mitigation process has been executed successfully.

The sequence of notifications shown in the SMS screenshots represents the complete communication flow of the AMI module. Initially, a normal system update is transmitted. This is followed by theft detection alerts when abnormal energy consumption is observed. Finally, a power cut-off confirmation message is generated after the relay disconnects the electrical supply. The time gap between messages demonstrates the actual operational sequence in which monitoring, detection, verification and mitigation occur.

Thus, the AMI module serves as the communication backbone of the proposed system by enabling real-time monitoring, event reporting, theft notification and confirmation of protective actions. It improves utility awareness, reduces response time and enhances the overall effectiveness of electricity theft risk assessment and mitigation.

6.3 Voltage and Current Analysis and Power Disconnection Results

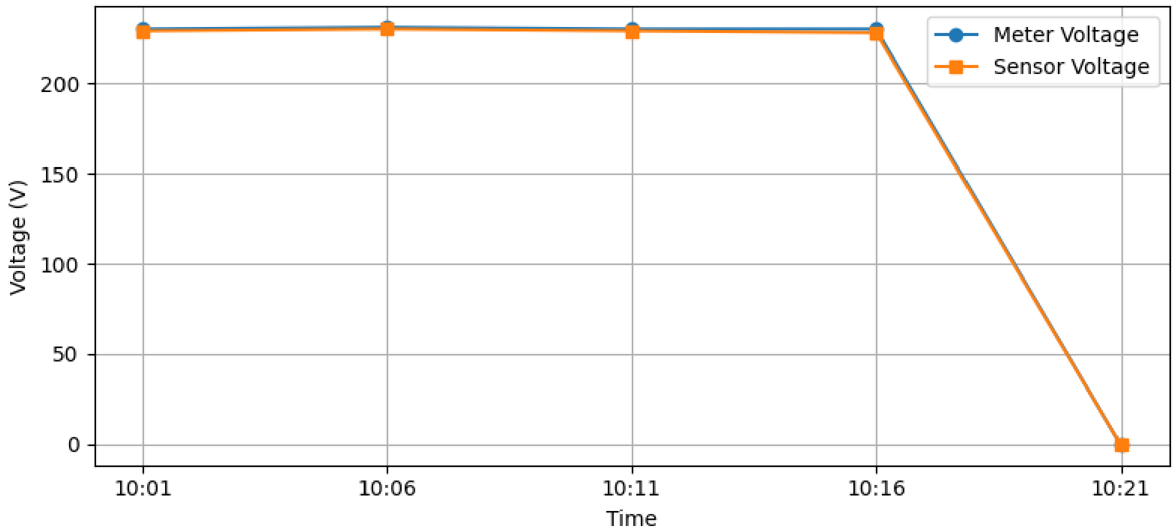

Figure 6. Voltage Variation Analysis of Meter and Sensor Readings

This graph in Figure 6 shows the voltage measured by the smart meter and the voltage measured by the external sensor. From 10:01 AM to 10:16 AM, both voltages remain stable around 228–231 V. The close agreement between the two measurements confirms that the supply voltage is healthy and the monitoring system is functioning correctly. Unlike current, voltage does not show a major variation during theft because illegal tapping mainly affects the current drawn from the system rather than the supply voltage level. Therefore, even when theft occurs, the voltage values remain nearly constant.

Once the AI module confirms the theft condition and issues a power disconnection command, the relay opens and isolates the consumer connection. Consequently, at 10:21 AM, both meter voltage and sensor voltage fall to 0 V. This indicates complete removal of the supply from the load side. The voltage graph therefore verifies the successful execution of automatic power cut-off after theft detection.

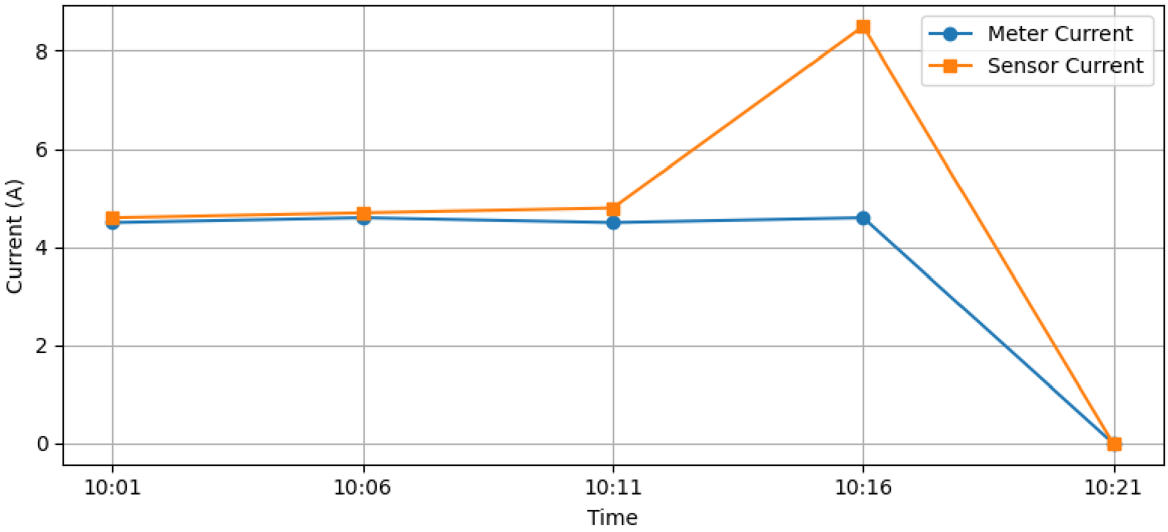

Figure 7. Current Variation Analysis of Meter and Sensor Readings

This graph in Figure 7 compares the current measured by the smart meter and the current measured by the external sensor. During the initial period (10:01 AM to 10:11 AM), both currents remain nearly equal, around 4.5–4.8 A. This indicates that all the current consumed by the load is passing through the energy meter and is being properly recorded. Therefore, the system considers the operation to be normal and no theft is detected.

At 10:16 AM, a significant deviation occurs. The meter current remains approximately 4.6 A, whereas the sensor current suddenly increases to about 8.5 A. This mismatch indicates that additional current is flowing through the line without being registered by the energy meter. Such a condition is characteristic of electricity theft through illegal tapping or bypassing of the meter. The AI module identifies this abnormal difference and classifies it as a theft condition.

After theft confirmation, the automatic disconnection mechanism is activated. At 10:21 AM, both meter current and sensor current drop to 0 A. This confirms that the relay or contactor has successfully disconnected the power supply, preventing further unauthorized energy consumption. The sharp drop to zero demonstrates the effectiveness of the proposed theft mitigation system.

7. CONCLUSION

This work presented an Electricity Theft Risk Assessment and Mitigation System that integrates Smart Meter, Internet of Things (IoT), Artificial Intelligence (AI), Advanced Metering Infrastructure (AMI) and Automatic Power Disconnection technologies to effectively detect and prevent electricity theft. The proposed system continuously monitors electrical parameters such as voltage, current, power and energy consumption through a smart meter and transmits the collected data using IoT communication. The AI-based analysis module evaluates real-time and historical consumption patterns to identify abnormal behavior and assess theft risk accurately. The AMI framework enables remote monitoring, data collection and communication between consumers and utility providers. When theft is detected, the system generates instant alerts and automatically disconnects the power supply to prevent further unauthorized energy consumption. The experimental results demonstrate that the proposed system provides accurate theft detection, rapid response, improved security, reduced non-technical losses and enhanced operational efficiency. Therefore, the proposed solution offers a reliable and intelligent approach for modern electricity theft management and revenue protection.

7.1 Future Enhancements

The proposed system can be further enhanced by incorporating advanced machine learning and deep learning algorithms to improve theft detection accuracy under complex operating conditions. Integration of blockchain technology can be considered to provide secure and tamper-proof storage of energy consumption data. The system may also be expanded to support large-scale smart city and smart grid applications through cloud-based centralized monitoring platforms. Future versions can include predictive analytics for forecasting theft risks before actual occurrences and enabling proactive preventive actions. Renewable energy monitoring, electric vehicle charging management and demand-side energy optimization features can also be integrated into the existing framework. Furthermore, the implementation of mobile applications with real-time dashboards, GPS-based location tracking of theft incidents and automated utility reporting can enhance system usability and operational effectiveness. These improvements will contribute to the development of a more intelligent, secure, scalable and efficient electricity theft detection and mitigation system.

REFERENCES

[1] K. S. Gowthaman and V. Gurukarthikeyan, "Smart Anti-Theft System for Energy Meters: Detection of Tampering and Power Tapping," *International Journal of Communication Networks and Information Security*, vol. 9, no. 3, pp. 503–509, 2017.

[2] S. McLaughlin, D. Podkuiko and P. McDaniel, "Energy Theft in the Advanced Metering Infrastructure," *Critical Information Infrastructures Security*, pp. 176–187, 2010.

[3] S. S. S. R. Depuru, L. Wang and V. Devabhaktuni, "Electricity Theft: Overview, Issues, Prevention and Detection Techniques," *Energy Policy*, vol. 39, no. 2, pp. 1007–1015, 2011.

[4] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen and X. Shen, "Energy-Theft Detection Issues for Advanced Metering Infrastructure in Smart Grid," *Tsinghua Science and Technology*, vol. 19, no. 2, pp. 105–120, 2014.

[5] N. Mohammad, A. Barua and M. Arafat, "A Smart Prepaid Energy Metering System to Control Electricity Theft," *International Conference on Power Electronics and Energy Systems*, pp. 1–5, 2015.

[6] H. Nizar, Z. Y. Dong and Y. Wang, "Power Utility Nontechnical Loss Analysis with Extreme Learning Machine Method," *IEEE Transactions on Power Systems*, vol. 23, no. 3, pp. 946–955, 2015.

[7] M. Jokar, N. Arianpoo and V. C. M. Leung, "Electricity Theft Detection in AMI Using Customers' Consumption Patterns," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 216–226, 2016.

[8] M. Faisal, M. A. Hannan, P. J. Ker and A. Hussain, "IoT-Based Smart Energy Monitoring System for Theft Detection," *International Journal of Electrical and Computer Engineering*, vol. 7, no. 6, pp. 3214–3222, 2017.

[9] A. Glauner, P. Valtchev, K. State and F. Bettinger, "The Challenge of Non-Technical Loss Detection Using Artificial Intelligence," *International Journal of Computational Intelligence Systems*, vol. 10, no. 1, pp. 760–775, 2017.

[10] M. Buzau, J. Tejedor-Aguilera, P. Cruz-Romero and A. Gómez-Expósito, "Detection of Non-Technical Losses Using Smart Meter Data and Machine Learning," *Energy and Buildings*, vol. 173, pp. 271–279, 2018.

[11] J. Zheng, D. W. Gao and L. Lin, "Smart Meters in Smart Grid: An Overview," *IEEE Green Technologies Conference*, pp. 57–64, 2018.

[12] P. Ghosh and S. Das, "Electricity Theft Detection Using Artificial Neural Networks," *International Journal of Energy Sector Management*, vol. 12, no. 4, pp. 632–645, 2018.

[13] Y. Xiao, Y. Wang, K. Lu and X. Wang, "Machine Learning-Based Detection of Electricity Theft in Smart Meter Networks," *IEEE Access*, vol. 7, pp. 184056–184068, 2019.

[14] A. Mahmood, N. Javaid and S. Razzaq, "A Review of Wireless Communications for Smart Grid," *Renewable and Sustainable Energy Reviews*, vol. 41, pp. 248–260, 2019.

[15] S. Hasan, M. K. Hasan and M. R. Islam, "Advanced Metering Infrastructure for Smart Energy Monitoring," *International Journal of Smart Grid*, vol. 3, no. 4, pp. 180–188, 2019.

[16] M. Amin, S. Khan and R. Ahmed, "Smart Meter Based Electricity Theft Detection System," *International Journal of Electrical Engineering*, vol. 26, no. 3, pp. 213–220, 2019.

[17] S. Singh and R. Sharma, "Electricity Theft Detection Using Deep Learning Techniques," *International Journal of Electrical Power & Energy Systems*, vol. 117, pp. 105624, 2020.

[18] M. Jindal, A. Singh and P. Kumar, "Artificial Intelligence Based Risk Assessment of Electricity Theft," *IEEE Access*, vol. 8, pp. 145870–145882, 2020.

[19] A. Nabil, M. Hossain and M. Rahman, “Smart Meter Security and Energy Theft Prevention in IoT Environments,” *Sensors*, vol. 20, no. 18, pp. 1–20, 2020.

[20] S. Sahoo and B. Mohanty, “Data Analytics for Electricity Theft Detection,” *Energy Reports*, vol. 6, pp. 2844–2853, 2020.

[21] R. Karthick, S. Suresh and P. Kannan, “Real-Time Electricity Theft Detection Using IoT and Cloud Computing,” *International Journal of Emerging Trends in Engineering Research*, vol. 9, no. 5, pp. 623–629, 2021.

[22] M. Ahmad, M. Naeem and A. Iqbal, “Hybrid Machine Learning Models for Electricity Theft Detection,” *Electric Power Systems Research*, vol. 196, pp. 107228, 2021.

[23] K. Ullah, A. Mahmood and M. Khan, “Smart Meter Data Analytics for Non-Technical Loss Identification,” *IEEE Access*, vol. 9, pp. 103421–103433, 2021.

[24] A. Prakash and S. Kumar, “IoT Enabled Smart Metering Framework for Energy Theft Monitoring,” *Journal of King Saud University – Engineering Sciences*, vol. 33, no. 8, pp. 560–568, 2021.

[25] S. Roy and P. Bhattacharya, “Consumer Load Pattern Analysis for Electricity Theft Detection,” *Energy Informatics*, vol. 4, no. 1, pp. 1–12, 2021.

[26] P. Sharma, A. Verma and D. Gupta, “AI-Based Electricity Theft Detection Framework for Smart Meter Systems,” *Sustainable Energy Technologies and Assessments*, vol. 52, pp. 102093, 2022.

[27] M. Al-Hawawreh, A. Al-Fuqaha and M. Guizani, “Intelligent Energy Monitoring and Theft Detection Using IoT,” *Internet of Things*, vol. 18, pp. 100482, 2022.

[28] H. Khan, M. Asif and S. Ali, “Automatic Power Disconnection System for Electricity Theft Prevention,” *IEEE Access*, vol. 10, pp. 88475–88486, 2022.

[29] S. Verma and R. Singh, “Machine Learning Approaches for Smart Meter Fraud Detection,” *Expert Systems with Applications*, vol. 201, pp. 117124, 2022.

[30] A. Rahman and M. Islam, “Real-Time Monitoring of Energy Consumption Using IoT Smart Meters,” *Measurement*, vol. 189, pp. 110524, 2022.

[31] K. Patel and V. Shah, “Electricity Theft Identification Through Data Mining Techniques,” *Energy Reports*, vol. 8, pp. 4512–4521, 2022.

[32] M. Noor, S. Ahmed and T. Khan, “Advanced Metering Infrastructure Based Theft Detection Framework,” *IEEE Access*, vol. 10, pp. 65421–65435, 2022.

[33] P. Kumar and R. Mishra, “Risk Assessment Model for Electricity Theft Detection,” *Sustainable Computing: Informatics and Systems*, vol. 35, pp. 100703, 2022.

[34] A. Sharma and N. Gupta, “Artificial Intelligence Techniques for Non-Technical Loss Reduction,” *Applied Energy*, vol. 315, pp. 118984, 2022.

[35] S. Prasad, R. Mishra and V. Patel, “AI and IoT Integrated Framework for Electricity Theft Monitoring,” *IEEE International Conference on Smart Energy Systems*, pp. 112–118, 2022.