Journal of Electrical Engineering and Automation (ISSN: 2582-3051)
www.irojournals.com/iroeea/

Smart IoT Energy Metering System with Real-Time Theft Detection and Prevention

Anbarasu L.[1], Kaviya S.[2], Geetha V.[3], Naresh S.[4], Saranraj M.[5]

[1-5]Electrical and Electronics Engineering, Erode Sengunthar Engineering College, Perundurai, Erode, India.

Email: [1]lanbarasu78@gmail.com, [2]kaviyas5858@gmail.com, [3]geetha5102004@gmail.com, [4]naresh.sinthai@gmail.com, [5]saransiruvai@gmail.com

Abstract

This article describes the design and development of a real-time, IoT-based smart energy meter for detecting electricity theft using a low-cost Arduino Uno, ESP8266 Wi-Fi module, and Blynk IoT platform, relying on threshold-based detection methods. In contrast to conventional energy meters that do not have tampering detection features, the designed system constantly checks for energy consumption using current sensors and monitors data to detect unauthorized power consumption. The uniqueness of this research is its cost-effective dual-load configuration that mimics both legal and illegal utilization scenarios, allowing real-time detection and instant notification through cloud-based dashboards. Experimental validation proves effective bypass scenario detection and distant notifications with negligible latency, making it ideal for smart grid integration in developing countries. The system improves energy accountability, enables remote monitoring, and offers a scalable solution to help fight electricity theft effectively.

Keywords: IoT, Smart Energy Meter, Power Theft Detection, Energy Efficiency, Real-time Monitoring, Internet of Things, Smart Grids, Tampering Detection.

1. Introduction

Electricity theft is a prevalent industrial-level activity causing billions of dollars in losses every year to power utilities across the globe. It is more common in most of the underdeveloped parts of the world, where infrastructure is compromised, consumption is

DOI: https://doi.org/10.36548/jeea.2025.2.005
Received: 13.05.2025, received in revised form: 16.06.2025, accepted: 03.07.2025, published: 15.07.2025

unmetered, and law enforcement practices are lackadaisical. Tampering, metering, and bypassing are the most prevalent types of theft that undermine the equitable distribution of power, raise the cost of doing business, and compromise the integrity of the overall power system. The denial of real-time insight into energy usage prevents utilities from detecting and reacting to theft in a timely manner. Conventional energy meters, such as electromechanical and simple digital meters, do not have theft detection, remote reading, or data analysis capabilities. Reading consumption manually is time-consuming, prone to errors, and impractical for very large electrical distribution networks. As the utilization of smart grids increases, robust and secure advanced metering infrastructure and real-time anomaly detection are required. The Internet of Things (IoT) has also played a significant role in this context by facilitating real-time data acquisition, wireless communication, and remote management of the power grid. IoT-enabled smart meters can continuously monitor voltage, current, and power consumption and send this data to cloud-based platforms for monitoring, analytics, and visualization. These technologies provide improved transparency, accurate billing, and real-time notifications whenever out-of-pattern behavior is detected.

Although there is much for IoT smart metering to gain from, existing solutions have the limitations of being costly to implement, requiring sophisticated infrastructure, and relying on the ubiquity of a stable internet connection or cloud processing. These limitations make them unsuitable for installation in rural or less-developed areas, where infrastructure is limited and technical know-how is in short supply. To counter these drawbacks, real-time low-cost electricity theft detection based on easily available hardware components, such as the Arduino Uno microcontroller, ESP8266 Wi-Fi module, current sensors, and the Blynk IoT platform, is discussed in this paper. The system enables the following:

- Real-time monitoring of home or industrial energy consumption,
- Real-time theft or tampering detection through differential current sensing,
- Real-time notification through a mobile dashboard during anomalies.

A double-load setup is employed to simulate stolen and actual power consumption patterns in such a way that the system can separate theft cases from normal consumption. It further demonstrates that inexpensive hardware can be leveraged to implement efficient theft detection systems without the need for expensive smart meters or complex AI-based models. Overall, this paper suggests a low-cost and scalable solution that will make energy metering systems responsive and smart. It aligns with the greater vision of utility revolution, smart grid

revolution, and energy accountability, and is therefore appropriate for developing economies that aim for non-technical loss reduction as well as assured power supply delivery.

2. Related Work

Recent technological innovations in IoT have refurbished the energy system significantly to make it smart, efficient, and secure. Tamilamuthan and Geetha [1] proposed an IoT system for enhanced energy management and electricity theft prevention using smart meters. Smart meters are the pillars of the modern grid system, enabling more open and reliable operation. To this end, Vijayaraja and Vidhya [2] analyzed how IoT-based systems enable data-driven, secure, and sustainable vehicle charging infrastructure for electric vehicles. The convergence of IoT has driven smart grid technology, following the argument presented by Dutta Pramanik et al. [3], which emphasized how critical the application of IoT is to guarantee real-time monitoring, on-demand load balancing, and optimal resource utilization. As remarkable as these technologies are, the security and privacy of users' data remain a concern. Marketyn et al. [4] and Club et al. [5] first identified the most obvious vulnerabilities of smart energy meters, such as privileged access and information leakage, and highlighted the necessity for secure encryption and secure communication protocols. While the convergence of IT and OT system design in energy platforms, investigated by Negi [6], indicates convergent digital energy systems, these infrastructures enable predictive maintenance as well as adaptive control. Mohamed et al. [7] also utilized artificial neural networks on IoT-based platforms for energy consumption optimization via intelligent pattern recognition and anomaly detection for sustainable processes. Cloud applications also play a more dominant role in holding extensive energy data. Manivannan et al. [8] demonstrated storage and key management methods focused on cryptographic security and decentralized management for IoT applications in the cloud. AbdelRaouf et al. [9] outlined privacy-protecting methods for smart grids and proposed the value-for-anonymity trade-off, which is key to gaining public confidence and regulatory approval to deploy IoT on a large scale. The review of previous works and their limitations is given in Table 1.

Table 1. Comparison of Related Works

Author	Method Used	Limitation	Proposed Model
Tamilamuthan et al [1]	Basic IoT smart meter	No tamper detection	Real-time tamper and theft detection with alerts
Mohamed et al. [7]	AI-based detection	High cost, complexity, data need	Lightweight, rule-based detection on microcontroller
Vijayaraja et al [2]	EV-oriented smart metering	Not focused on theft detection	Theft-specific detection with remote monitoring

3. Working Model

The intended system is an Arduino-powered smart energy monitoring and control system with power consumption monitoring and remote appliance control. The core of the system is the Arduino Uno, which acts as the central microcontroller and controls the input, processing, and data transmission of all devices. Two electric bulbs are connected to the system, each paired with a current sensor in series. These sensors continuously read the electric current consumed by each bulb and output analog values to the Arduino Uno. The microcontroller measures real-time power consumption from this output. The real-time power consumption reading of each load (i.e., bulbs) is displayed on the LCD, which is interfaced with an I2C module. Using the I2C module, wiring and communication are simplified, and updating the display is performed more efficiently with fewer I/O pins.

3.1 Materials Used

Table 2. Components Used in the Proposed Model

Component	Model Name	Function
Microcontroller	Arduino Uno R3	Regulates communication, logic, and sensors.
Current Sensor	ACS712 5A Module	Detects the current in both normal and stolen lines in real time.
Wi-Fi Module	ESP8266 NodeMCU	Data is sent to the IoT dashboard.

Display Unit	LCD 16x2 with I2C	Displays current values and alerts for theft.
IoT Platform	Blynk App	Allows for remote notifications and monitoring
Power Supply	5V USB Adapter	Supplies power to sensors and Arduino
Load Device	230V AC Bulbs	Simulates the use of power both legally and illegally (bypass).

Table 2 shows the components used in the proposed model and Figure 1 illustrates the block diagram of the proposed model for remote monitoring and control, the system incorporates a Wi-Fi module (e.g., ESP8266) so that the Arduino can access the internet. With the internet connection, users can open a web or mobile interface to remotely monitor power usage and control electrical devices (bulbs or plugs). Additionally, a plug is shown in the diagram as a controllable output device.

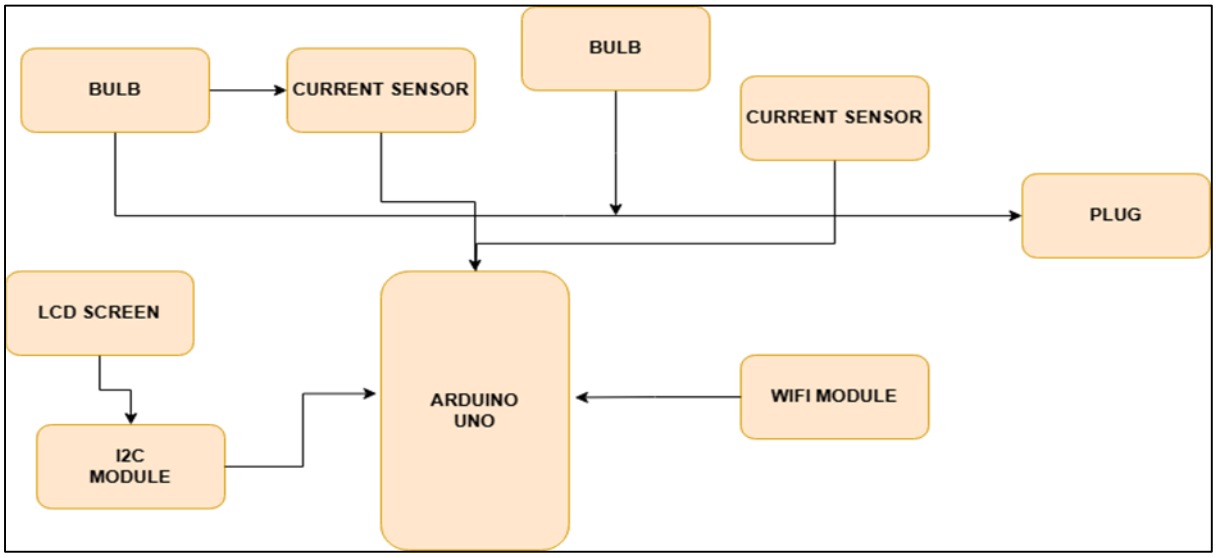


Figure 1. Block Diagram of the Proposed System

Based on predefined conditions or user commands received over Wi-Fi, the Arduino can turn the plug (or the connected load) on or off, making the system suitable for smart home automation and energy-saving applications. In general, the system continuously reads ongoing values, computes consumption, displays the results, and supports real-time remote control, thus providing an efficient solution for energy monitoring and smart switching in an office or home setting.

4. Proposed Work

The system's sequential detection logic is shown in Figure 2, which begins with sensor and server connection initialization and continues with ongoing real-time current value monitoring. An alert is triggered if a current deviation between the legal and illegal lines is detected. The suggested system will detect electricity theft in real time through smart metering infrastructure and IoT-based analysis.

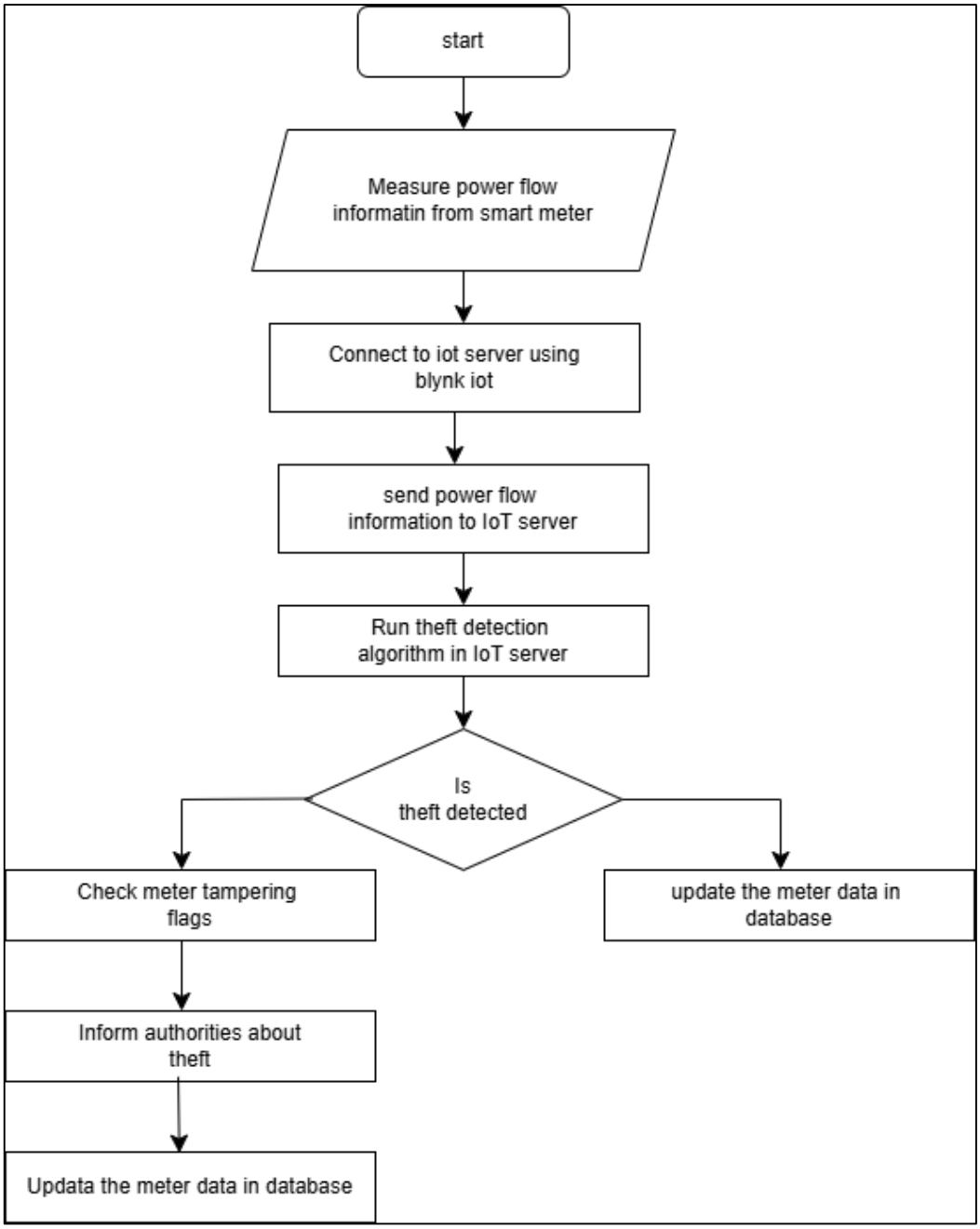


Figure 2. Flowchart of the Model

It starts with real-time power flow data monitoring by a smart energy meter placed on the consumer side. The meter records real-time energy consumption and sends it to an IoT server through the Blynk IoT platform. When connected to the IoT server, the smart meter sends electricity usage data over an encrypted channel. The server also runs a theft detection algorithm, which periodically sifts through input data for anomalies. This type of algorithm compares existing patterns of actual usage to modeled patterns of usage and identifies anomalies as possible indicators of theft or tampering.

If there is no theft, the system simply updates meter records in the central database for accurate and continuous records. However, if any anomalous behavior is identified, the system triggers a thorough investigation by checking for tampering evidence such as unusual consumption dips or attempts to bypass or reverse power flow. After the system detects tampering or electricity theft, it alerts the concerned authorities with evidence. Meanwhile, the system also saves the meter reading to the database for consumption history integrity and subsequent follow-up investigation or enforcement. The following pseudocode can be used to simplify the Arduino's core theft detection logic:

```
IF (Sensor1_Current == 0 AND Sensor2_Current > Threshold)
   THEN Trigger Theft Alert
ELSE
   Log Normal Usage
END IF
```

This intelligent energy metering system, therefore, offers a real-time, scalable, and automated platform for the identification and reporting of electricity theft, maximizing grid security and utility management through timely action and precise data recording. This system's theft detection algorithm is based on comparing two existing sensors. A theft alert is triggered if Sensor 2 (which is connected to the illegal bypass line) detects current while Sensor 1 (the legal line) shows none or significantly less. For sensor calibration errors, a threshold margin of 5% deviation is regarded as typical. Any persistent departure from this is considered questionable.

5. Results and Discussion

The envisioned electricity theft detection system was implemented successfully based on the Arduino Uno microcontroller, current sensors, ESP8266 Wi-Fi module, and a 16x2 LCD

display. The circuit structure comprised two loads: one loaded normally (lawful use) and another loaded bypassing the metering point to represent unlawful use (theft load). The physical prototype duplicated the circuit diagram fairly accurately, revealing functional accuracy between the design concept and hardware realization. Figure 3 shows the circuit diagram of the proposed model.

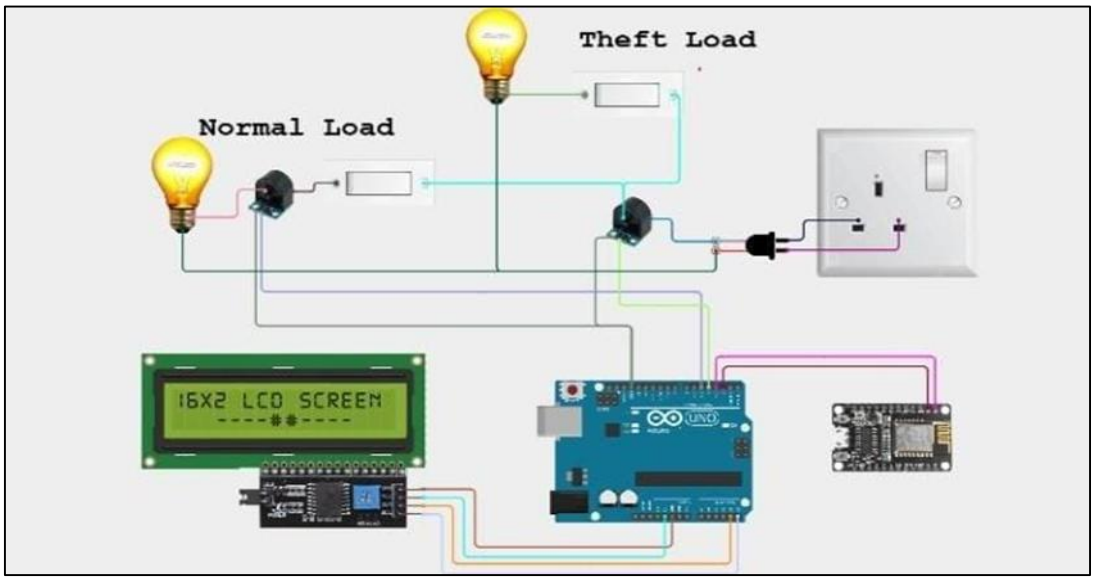


Figure 3. Circuit Diagram of the Designed Model

Upon switching on the system, the current sensors kept checking the actual power usage of the normal and theft circuits in real time. When the normal load alone was being used, the system reported typical power usage on the LCD, and no alarm was issued. However, as soon as the theft load was activated, i.e., power consumed without going through the main switch, the system detected the anomaly in no time. This difference was calculated by the Arduino Uno and sent to the Blynk IoT server via the ESP8266 module.

The LCD displayed "Theft Load Detected" in real time, indicating that the algorithm was able to distinguish between an authorized and an unauthorized load. At the same time, this event was propagated to the cloud server, where it was logged as an anomaly and made available through the Blynk dashboard interface. This remote notification function facilitates rapid response from utility providers or administrators. The system was also found to be consistent in different test situations that entailed single and dual load combinations, with online updates in real-time and low latency. The Wi-Fi connection remained consistent throughout, and the utilization of the ESP8266 provided smooth communication between the

hardware configuration and the online server. Figure 4 demonstrates the hardware design of the proposed work.

Figure 4. Hardware Kit of the Proposed Model

The system, as a whole, exhibited:

- Correct identification of power theft incidents,
- Real-time reporting and alerting through LCD and IoT dashboard,
- Consistent remote monitoring and database updating,
- Low-cost and scalable architecture that is appropriate for use in smart grid deployments.

This prototype verifies that the combination of smart metering and IoT-based analytics has the potential to greatly improve transparency and accountability in energy distribution networks. The speed of detection and understanding of visual warnings make this model exceptionally beneficial in energy-sensitive and tamper-vulnerable environments. Figure 5 shows the current readings from Sensor 1 (Normal Line) and Sensor 2 (Theft Line) over time. Security protocols like TLS or device authentication were not used in this prototype, despite the fact that the suggested system uses the Blynk IoT platform to transmit data. Multi-factor authentication and encrypted communication for dashboard access are potential future improvements.

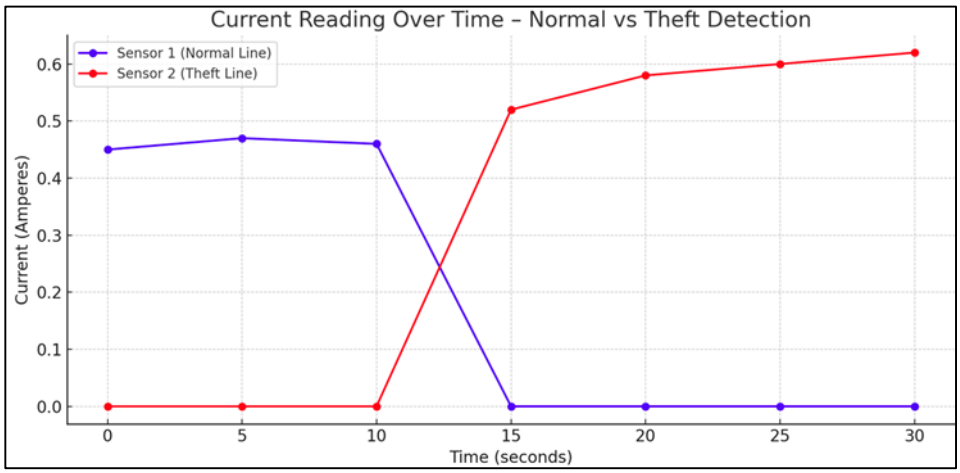
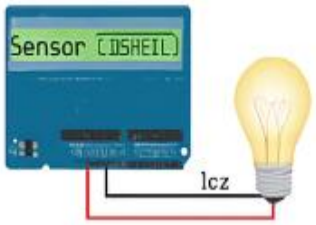
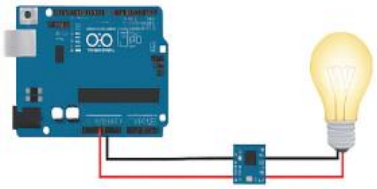
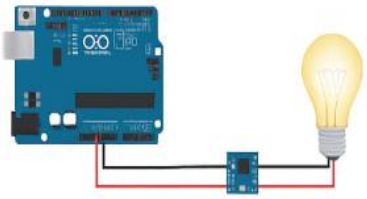
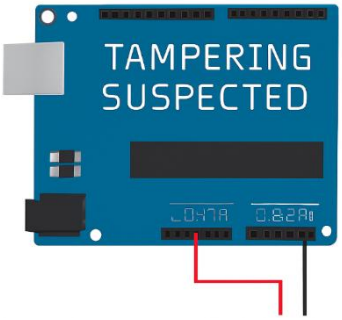


Figure 5. Graph Showing Current Readings from Sensor 1 (Normal Line) and Sensor 2 (Theft Line) Over Time

Table 3. Test Cases and Observations

Test Case	Setup Description	Expected Behaviour	Observed
Normal Operation	Single load connected through legal line	Accurate current reading 	Values displayed on LCD & Blynk: No alert triggered
Direct Bypass Theft		Sensor 2 detects current; Sensor 1 shows none 	"Theft Detected" shown in LCD and in Blynk

Phase Shorting Theft		Abnormal current inconsistency across sensors 	Alert triggered due to imbalance detection
Meter Door Tampering	Lid opened (Magnetic tamper switch triggered) 	Physical tamper sent 	Tamper Detected

6. Conclusion

IoT-enabled smart energy meters with stolen unit detection provide a complete solution to the drawbacks of traditional energy metering systems. Specifically, they address power theft detection and utilization anomalies. With real-time data acquisition, threshold logic, and cloud connectivity monitoring, the system enhances the measurement accuracy of energy consumption, prevents economic loss through exploitation, and facilitates efficient energy management. One advantage of smart systems is their ability to provide real-time alerts to users and utility companies, allowing them to learn and act the instant cheating or stealing is attempted. In the long run, this smart process not only ensures optimal utilization of energy but also promotes clean billing, a secure grid infrastructure, and environmentally friendly lifestyles. Their installation brings us one step closer to the smart, intelligent energy grids that will enable the evolution of a more efficient and intelligent energy infrastructure.

References

[1] Tamilamuthan, R., and B. T. Geetha. "IoT-Driven Solutions for Efficient Energy Management and Theft Prevention for Smart Meter." Available at SSRN 5086732 (2024).

[2] Vijayaraja, L., and D. Vidhya. "IoT-Driven Innovations for Sustainable and Secure Electric Vehicle Transportation." In 2025 International Conference on Computing and Communication Technologies (ICCCT), IEEE, (2025): 1-4.

[3] Dutta Pramanik, Pijush K., Bijoy K. Upadhyaya, Ajay Kushwaha, and Debashish Bhowmik. "Harnessing IoT: Transforming Smart Grid Advancements." IoT for Smart Grid: Revolutionizing Electrical Engineering (2025): 127-174.

[4] Marketyn, S., C. Alex, and B. Ellis. "Data Security and Privacy Concerns in IoT-Driven Smart Energy Meter Systems." Curr Res Next Gen Mater Eng 1, no. 1 (2025): 01-07.

[5] Club, A., C. Alex, and B. Ellis. "Understanding the Basics: How IoT Revolutionizes Smart Energy Meter Systems." Curr Res Next Gen Mater Eng 1, no. 1 (2025): 01-07.

[6] Negi, Mansi. "Towards the integration of IT/OT technologies in Electricity Based Digitalized Energy Systems." (2024).

[7] Mohamed, Azza, Ibrahim Ismail, and Mohammed AlDaraawi. "IoT-Driven Intelligent Energy Management: Leveraging Smart Monitoring Applications and Artificial Neural Networks (ANN) for Sustainable Practices." Computers 14, no. 7 (2025): 269.

[8] Manivannan, I. Sivaprasad, A. Andrew Roobert, and N. Muthukumaran. "A Detailed Analysis of Cloud Storage and Key Management Techniques in IoT Driven Smart Grids." In 2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT), vol. 1, IEEE, (2024): 1786-1791.

[9] AbdelRaouf, Hussien, Michael Long, Paul Tran, Luna Baral, Zuha Khan, Mohamed Mahmoud, Mostafa M. Fouda, and Mohamed I. Ibrahem. "Privacy Preservation Techniques in Smart Grids: Balancing Security and Utility in IoT-Driven Environments." In 2024 2nd International Conference on Artificial Intelligence, Blockchain, and Internet of Things (AIBThings), IEEE, (2024): 1-6