

DESIGN AND IMPLEMENTATION OF AN IOT-BASED SMART ENERGY METER WITH ANTI-THEFT PROTECTION

Dr.Shaik.Bajid vali^{1*}, K. Madiha^{2*}, K. Pavan Kumar Reddy³, P. Vyshnavi⁴,
M.Venkateswarulu⁵

^{1*} Professor, ECE, Chaitanya Bharathi Institute of Technology, Proddatur, India, 516360

^{2*} Student, ECE, Chaitanya Bharathi Institute of Technology, Proddatur, India, 516360

³ Student, ECE, Chaitanya Bharathi Institute of Technology, Proddatur, India, 516360

⁴ Student, ECE, Chaitanya Bharathi Institute of Technology, Proddatur, India, 516360

⁵ Student, ECE, Chaitanya Bharathi Institute of Technology, Proddatur, India, 516360

^{1*} Corresponding Author E-mail: bajid.vali.ece@cbit.edu.in

^{2*} Corresponding Author E-mail: kandukurumadiha@gmail.com

ABSTRACT:

Electricity is also extensively applied in houses, educational institutions, and factories, and it is significant to control electricity use and avoid theft of electricity. The project under discussion is called Design and Implementation of an IoT-Based Smart Energy Meter with Anti-Theft Protection, which aims at the quantitative measurement of electricity consumption, as well as detection of illegal use of power. The hardware elements used in the system will consist of rudimentary components including an energy meter, NODEMCU, IR sensor, LCD display and a buzzer. The IR sensor is fitted by a location close to the energy meter to capture the blinking pulses that are used to show the consumption of energy. The NODEMCU counts and processes these pulses and computes the total amount of electricity used. The information gathered is linked to the internet via Wi-Fi and thus can be monitored remotely. It has an LCD display to show the real time use of energy easily to the user. The system will monitor abnormal and unanticipated power consumption in order to avoid theft of electricity. A buzzer is used as an alert in case such conditions are sensed. The suggested system is cheap, simple to install, and it can be applied to effective energy monitoring and preventing theft.

KEYWORDS: IoT, Smart Energy Meter, Electricity Theft Detection, NODEMCU, IR Sensor, Energy Monitoring, Anti-Theft System

INTRODUCTION:

The fast development of smart cities requires proper, real-timed observation of energy and water use to decrease its wastage and operational expenses. The conventional meter systems use manual readings and therefore have delays and billing errors and lack of user consciousness. The proposed project compiles and helps solve these problems by coming up with an IoT-based smart energy metering system with anti-theft abilities through the use of NODEMCU. The system keeps a constant track of the energy consumption rate by use of an energy meter and unauthorized usage by an IR sensor. The data is sent to the IoT in real time, and the alert is given to the user with the help of LCD and a buzzer. The offered system increases transparency, eliminates the theft of power, and allows to effectively manage the utilities in smart city conditions [1]. The growing demand in global energy and climate change issue demand smarter and efficient energy management systems. The conventional energy infrastructure does not have real-time intelligence and does not offer practical insights on optimization and decisions. Smart meters can solve this issue by constantly gathering comprehensive consumption data on the energy network. The paper summarizes the application of Smart meter data to produce Business Intelligence in the Smart Energy system using IoT, cloud, and AI technologies. It brings to focus analytics architectures, computational stacks and AI-driven applications made possible by smart meters. The major contribution to the paper is to recognize research gaps and areas that next-generation smart metering and intelligent energy system are heading to in the future [2]. Increasing integration of renewable and distributed sources of energy has rendered the flow of power in smart grids to be two-way/bidirectional and even more difficult to control. Traditional power meters are not highly synchronized in time which results into lack of accuracy in monitoring of energy flows and inefficient management of the energy flows. This paper answers the question of providing the synchronisation of sensing devices by examining the current ways of satellite- and network-based synchronisation. It suggests the application of the IEEE 1588 Precision Time Protocol (PTP) in order to get effective time alignment in smart power meters. Time- synchronized meters are installed in a microgrid and operated in an automatic control station. The positive outcomes of the experiment prove the efficiency of using PTP to facilitate efficient monitoring and superior smart grid energy control [3]. Smart meters are used in the low voltage energy delivery systems although it is still a big challenge to detect fault or abnormal meters. The conventional inspection practice is not only time-consuming but also expensive and cannot be applied in mass smart grid deployment. This paper suggests an error estimation method of the smart meter based on orthogonal matching pursuit and Bollinger Band-based data filtering. Data of abnormal meter is initially detected and eliminated and a recursive model is used to estimate the errors in meters. The experimental findings prove to be accurate better than 90 percent practical accuracy with a low level of line loss. The suggested method also has fewer error values compared with both classical and machine-

learning methods, which presents an efficient solution to a large smart grid system [4]. Smart meters produce fine measurement data which is essential to observe smaller distribution systems (voltage). Nonetheless, detecting the anomalies like non-technical loss and high-impedance faults cannot be easily detected because of the inconsistency between the methods of detecting them. This paper suggests statistical score called the Anomaly Intensity Index, which is made out of smart meter readings. The index rates the local and system-wide information to identify and spot unusual operating conditions. It ranks the consumers in terms of the deviation level which facilitates specific research. Through experiment, it has been demonstrated that small abnormal demands are correctly detected at a low demand of 0.2 kW per phase with an error in estimating the energy less than 1 percent [15]. The networks of Advanced Metering Infrastructure (AMI) are based on high-quality data transmission, low energy consumption, and long network lifespan requirements. Single-parent routing in AMI cannot balance reliability in transmissions and energy efficiency, and the multi-parent routing determines unwarranted overheads in energy consumption. The proposed implication of this trade-off in this paper is that the paper will suggest a Trilateral Smart Switching (TSS) algorithm. The algorithm switches between two modes single-parent and multi-parent transmission dynamically and determines the right channels of communication depending on network and channel conditions. A combination of Zigbee and cognitive radio communication gives TSS the workload balancing and adaptive transmission. By simulation, it can be observed that AMI networks have better packet delivery rate, lower latency, and longer network life [10]. The intensive use of smart electric meters in smart grids has raised concerns on cyber security and faithfulness of data. Smart meters are open to cyber-attacks due to the fact that remote monitoring is carried out by the use of network communication protocols. Nevertheless, there is experimental analysis of the real life behavior of commercial smart meters with such attacks. This paper experimentally examines the robustness of commercial grade smart meters to the most prevalent cyber security attacks. Experiments were carried out in real laboratories using meters of outstanding manufacturers and standardized network gear. The findings show that cyber-attacks have the potential to cripple or entirely halt power-usage data reporting and therefore more robust security mechanisms must be integrated in smart metering systems [11].

BACKGROUND AND RELATED WORK:

Raza *et al.* (2023) reviewed the role of smart meters in Smart Energy systems, focusing on Business Intelligence applications using IoT, cloud, and AI analytics across sensing to fog layers. The study highlighted advanced data collection, computational stacks, and intelligent energy management use cases. However, the work remains primarily a survey without proposing an implementation or performance evaluation model. It does not address real-time hardware integration, security, or energy theft detection. Practical challenges such as communication latency, cost constraints, and edge-level decision-making are also not explored. These gaps motivate the need for an implemented IoT-based smart metering system with real-time monitoring, security, and efficient data utilization [2]. Hseiki *et al.* (2023) presented a secure and resilient smart energy meter design addressing cybersecurity and data integrity challenges in smart grids. The work analysed cyber-attack surfaces and proposed a multi-level security architecture covering hardware, communication, and data protection. LoRaWAN and unidirectional communication were used to mitigate threats such as DDoS attacks, data manipulation, and energy theft. However, the study focuses mainly on security architecture and lacks detailed performance evaluation under real-time operational conditions. Integration with real-time consumption monitoring, user-side analytics, and cost-effective implementation is not explored. These gaps highlight the need for a practical IoT-based smart meter that combines security, real-time monitoring, and efficient energy management [5]. Sushma *et al.* (2022) proposed a unified wireless metering system for simultaneous water and energy monitoring in smart city environments using LPWAN technology. The system enables real-time consumption monitoring, remote control, and improved customer engagement by integrating water flow sensors and energy meters. Experimental results demonstrated accurate readings and reliable communication between meters. However, the system relies on trial-and-error interoperability and does not focus on security, cyber-attack resilience, or advanced anomaly detection. Issues such as energy theft detection, data analytics, and intelligent decision-making are minimally addressed. These gaps motivate the need for a secure, intelligent IoT-based smart metering system with enhanced monitoring and protection features [1]. Biswas *et al.* (2024) presented an extensive review of smart grids for sustainable energy management, covering grid components, renewable energy integration, AI-driven analytics, cybersecurity, and privacy issues. The study highlights key challenges such as renewable energy intermittency, cyber threats, and large-scale electric vehicle integration. It emphasizes the role of AI and data analytics in improving grid efficiency, reliability, and energy optimization. However, the work remains a high-level survey without experimental validation or hardware implementation. Practical deployment issues at the smart meter level are not deeply explored. These gaps indicate the need for an implemented, secure IoT-based smart metering system with real-time monitoring and intelligent control [12].

PROBLEM STATEMENT:

The increasing adoption of smart grids and smart city infrastructures has created a strong need for reliable and intelligent energy monitoring systems. Although existing studies discuss smart meters, IoT integration, cybersecurity architectures, LPWAN communication, data analytics, and privacy protection, most of these works are limited to surveys, conceptual

frameworks, or network-level designs. Many proposed approaches do not include real-time hardware implementation, system-level integration, or experimental performance evaluation under practical operating conditions. Current solutions often focus on individual aspects such as data analytics, security, or communication, without offering a complete and integrated smart metering system. Important challenges such as real-time energy consumption monitoring, secure data transmission, energy theft detection, communication latency, and edge-level decision-making are not adequately addressed. In addition, issues related to cost-effective deployment, user-side monitoring, and scalable implementation suitable for real-world environments remain largely unexplored. As a result, there is a clear gap in the development of a practical IoT-based smart energy metering system that combines real-time monitoring, security, and intelligent data utilization. Addressing these limitations requires an implemented solution that integrates hardware and software, supports secure and efficient communication, enables theft detection and anomaly monitoring, and provides reliable energy management for modern smart grid applications.

LITERATURE REVIEW (EXISTING SYSTEM & PROPOSED SYSTEM)

EXISTING SYSTEM:

From the literature survey, the existing smart energy metering systems are mainly designed around IoT-based monitoring, cloud connectivity, and data analytics for smart grid applications. Many studies focus on integrating smart meters with IoT platforms to enable remote monitoring, automated billing, and energy usage analysis. Advanced communication technologies such as LPWAN and LoRaWAN are used to ensure long-range and low-power data transmission. Some research works also propose cybersecurity frameworks to protect smart meters from cyber-attacks, data manipulation, and unauthorized access. Several survey-based studies highlight the role of Artificial Intelligence and Business Intelligence tools in improving energy efficiency, demand forecasting, and grid optimization. Other works address privacy protection through encryption methods and differential privacy techniques to secure user energy data. A few systems combine water and electricity monitoring for smart city applications, enabling unified data collection and remote access. However, most existing systems remain conceptual, survey-based, or limited to specific features such as security or communication. Practical hardware implementation, real-time performance validation, integrated energy theft detection, and cost-effective deployment at the consumer level are not comprehensively addressed. As a result, existing systems lack a fully integrated, real-time, and secure smart metering solution suitable for large-scale practical implementation.

PROPOSED SYSTEM:

The proposed project, “Design and Implementation of an IoT-Based Smart Energy Meter with Anti-Theft Protection,” offers significant improvements over existing systems discussed in the literature survey. While many existing systems focus mainly on data monitoring, communication, or security separately, the proposed block diagram integrates all essential features into a single practical and implementable model. In the given block diagram, the Energy Meter measures power consumption, and the IR Sensor detects meter pulse signals to calculate energy usage accurately. The NodeMCU acts as the central controller, processing real-time data and sending it to the IoT platform through built-in Wi-Fi. Unlike many survey-based models, this system provides actual hardware-level implementation with real-time monitoring. The addition of a Buzzer enhances anti-theft protection by giving immediate alerts when abnormal activity or meter tampering is detected. The LCD Display allows users to view live energy consumption locally without depending only on cloud access. The Power Supply ensures stable operation of all components. Compared to existing systems, this project combines real-time monitoring, IoT connectivity, theft detection, local display, and alert mechanisms in a cost-effective and practical setup. It moves beyond theoretical frameworks and provides a working prototype suitable for real-world smart grid applications.

SYSTEM ARCHITECTURE:

The proposed architecture consists of an Energy Meter, IR sensor, NodeMCU, LCD display, buzzer, power supply, and IoT platform. The energy meter measures electricity consumption, and the IR sensor detects the blinking pulses from the meter to calculate the number of units consumed. The NodeMCU acts as the main controller, processing the pulse data and sending real-time energy information to the IoT cloud through Wi-Fi. The LCD displays current consumption locally for user reference. The buzzer provides alerts during abnormal conditions or possible energy theft. The power supply ensures stable operation of all components in the system.

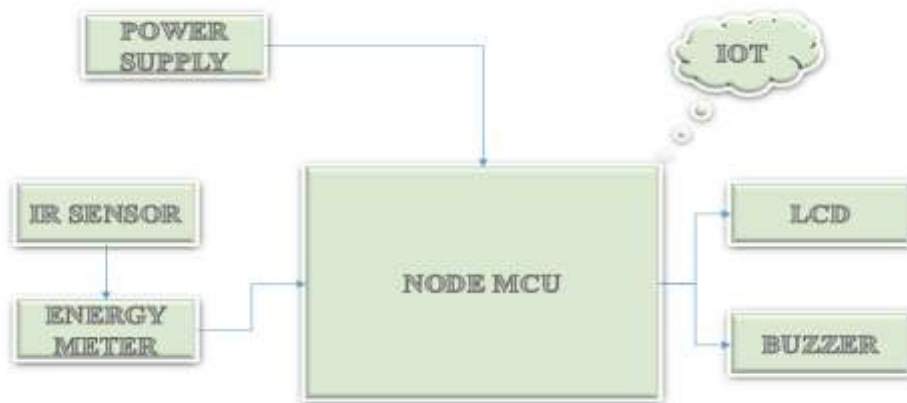


FIG: 1 SYSTEM ARCHITECTURE
SYSTEM MODULES:
ENERGY METER



FIG: 2 ENERGY METER

The energy meter is the primary sensing device used to measure electrical energy consumption. It generates a blinking LED output, where each blink corresponds to a fixed amount of energy used (usually in units or pulses per kWh). This output serves as the input signal for monitoring power usage. The energy meter ensures accurate measurement of electricity consumption in real time. It forms the foundation of the entire system by providing reliable consumption data.

IR SENSOR



FIG: 3 IR SENSOR

The IR (Infrared) sensor is used to detect the blinking LED of the energy meter. Each detected blink represents a unit of electricity consumption. The sensor converts these optical pulses into electrical signals that can be processed by the controller. It enables non-intrusive measurement without modifying the internal circuitry of the energy meter. This makes the system safe, simple, and cost-effective.

NODEMCU (ESP8266)



FIG: 4 NODEMCU (ESP8266)

The NODEMCU acts as the main controller of the system. It receives pulse signals from the IR sensor and calculates the total energy consumption based on the number of pulses detected. With its built-in Wi-Fi module, it sends real-time energy usage data to the cloud for remote monitoring. The NODEMCU also analyses usage patterns to detect abnormal or theft conditions. It controls the LCD display and activates the buzzer during alerts.

LCD DISPLAY



www.ijiemr.org | 2(12)19082

FIG: 5 LCD DISPLAY

The LCD display provides real-time visual feedback of electricity consumption. It shows information such as total units consumed and system status. This allows users to monitor their energy usage easily without accessing the internet. The display improves user interaction and awareness of power consumption. It helps in promoting energy conservation by making usage data clearly visible.

BUZZER



FIG: 6 BUZZER

The buzzer acts as an alert and warning device in the system. It is activated when abnormal power usage or electricity theft is detected. The buzzer provides immediate audio notification to the user or authorities. This quick alert mechanism helps prevent prolonged electricity theft or over-consumption. It enhances the safety and security of the energy monitoring system.

POWER SUPPLY UNIT



FIG 7: POWER SUPPLY UNIT

The power supply unit provides regulated voltage to all hardware components. It ensures stable and reliable operation of the system. Proper power regulation protects components from damage. Continuous operation is maintained during monitoring.

EMBEDDED C PROGRAMMING:

Embedded C is a specialized extension of the C programming language designed specifically for programming microcontrollers and other embedded systems. Unlike standard C, Embedded C provides features for directly interacting with hardware, such as addressing specific memory locations, performing fixed-point arithmetic, and handling input/output hardware directly. Embedded systems themselves are dedicated devices created to perform specific tasks, comprising both hardware and integrated software (firmware). Embedded C is widely used to program microprocessors and microcontrollers efficiently, requiring fewer system resources compared to lower-level languages like assembly.

The language also includes unique data types and keywords tailored for hardware interaction. For instance, SBIT and SFR are used to access special function registers in memory. Embedded C facilitates direct communication with sensors, actuators, and other I/O devices, making it ideal for real-time control applications. Programs written in Embedded C can be compiled using various compilers such as Keil, SPJ Compiler, and Embedded GNU C Compiler. Embedded systems can range from simple devices to complex machinery, and Embedded C is employed in everyday electronics such as air conditioners, printers, and mobile phones.

ARDUINO'S PROGRAMMING CONCEPT:

Arduino is a user-friendly platform designed for creating interactive physical computing projects. Built around a microcontroller, Arduino provides a direct interface with the physical world, allowing devices to sense inputs from switches, sensors, or other components and control outputs such as motors, lights, or displays. Its integrated development environment (IDE) simplifies programming and uploading code to the board. Arduino boards can operate independently or communicate with computer software for more advanced applications. They are available as pre-assembled or DIY kits, and the open-source design allows anyone to download and modify the hardware and software. The Arduino programming language is derived from Wiring and inspired by the Processing multimedia framework, enabling intuitive coding for interactive objects and physical computing devices. This combination of simplicity, flexibility, and accessibility makes Arduino widely used in robotics, automation, and IoT projects.

FIG 8: ARDUINO IDE

LIMITATIONS AND FUTURE SCOPE:

Although the proposed IoT-based smart energy meter with anti-theft protection provides real-time monitoring and basic security features, it has certain limitations. The system mainly depends on Wi-Fi connectivity, which may not be reliable in areas with poor internet coverage. Any network failure can interrupt real-time data transmission to the cloud. The current design uses an IR sensor to detect meter pulses, which may be affected by environmental factors such as dust or improper alignment. The anti-theft mechanism is based on abnormal pulse detection, but it may not identify all advanced tampering techniques. In addition, the system is designed for small-scale implementation and may require modification for large-scale deployment in smart grid environments. In the future, the system can be enhanced by integrating advanced machine learning algorithms for accurate energy theft detection and anomaly analysis. GSM communication modules can be added to improve long-range connectivity. Mobile application support can provide better user interaction and billing management. Cloud-based data analytics can help in load prediction and demand management. Integration with renewable energy systems and smart home automation can further improve efficiency and scalability, making the system more suitable for modern smart city applications.

RESULT:

The proposed IoT-Based Smart Energy Meter with Anti-Theft Protection was designed and implemented to monitor electricity consumption and detect abnormal usage conditions. The system was tested under different load conditions to evaluate its performance in real-time monitoring and theft detection. During normal operation, the energy meter produced LED pulses proportional to the connected electrical load. The IR sensor accurately detected these pulses and forwarded them to the NODEMCU. The controller successfully counted the pulses and calculated the total energy consumption. The measured values were displayed on the LCD in real time and were also transmitted to the IoT platform through Wi-Fi without noticeable delay. When additional loads were suddenly connected or abnormal consumption patterns were introduced, the system identified these conditions as unusual power usage. The NODEMCU triggered the buzzer immediately, providing an audible alert. This demonstrated the effectiveness of the anti-theft mechanism in identifying over-consumption and possible electricity theft scenarios. The results indicate that the proposed system provides reliable and accurate energy monitoring while reducing the need for manual meter reading. The integration of IoT technology enables continuous remote supervision of electricity usage. Overall, the system improves energy management, enhances security against electricity theft, and supports efficient utilization of electrical power.

CONCLUSION:

We concluded that, this project successfully provides real-time electricity monitoring and effective detection of abnormal power usage. The system reduces manual effort, improves billing accuracy, and enhances security against electricity theft. By using IoT technology, remote monitoring and instant alerts are achieved efficiently. In the future, the system can be

enhanced by integrating mobile applications, advanced data analytics, and automatic power disconnection features for improved control and large-scale deployment.

REFERENCES:

- [1] N. Sushma, H. N. Suresh, J. M. Lakshmi, P. N. Srinivasu, A. K. Bhoi and P. Barsocchi, "A Unified Metering System Deployed for Water and Energy Monitoring in Smart City," in *IEEE Access*, vol. 11, pp. 80429-80447, 2023, doi: 10.1109/ACCESS.2023.3299825.
- [2] M. H. Raza, Y. M. Rind, I. Javed, M. Zubair, M. Q. Mehmood and Y. Massoud, "Smart Meters for Smart Energy: A Review of Business Intelligence Applications," in *IEEE Access*, vol. 11, pp. 120001-120022, 2023, doi: 10.1109/ACCESS.2023.3326724.
- [3] R. Morello, G. Fulco, S. Mukhopadhyay, L. Fabbiano and C. De Capua, "Time Synchronized Power Meters for Advanced Smart Distribution of Energy in Smart Grids," in *IEEE Sensors Journal*, vol. 24, no. 19, pp. 30909-30919, 1 Oct.1, 2024, doi: 10.1109/JSEN.2024.3445494.
- [4] F. Liu and H. Huang, "Smart Meter Error Estimation in Topological Low Voltage Energy System," in *IEEE Access*, vol. 12, pp. 147422-147437, 2024, doi: 10.1109/ACCESS.2024.3471669.
- [5] Hseiki, A. M. El-Hajj, Y. O. Ajra, F. A. Hija and A. M. Haidar, "A Secure and Resilient Smart Energy Meter," in *IEEE Access*, vol. 12, pp. 3114-3125, 2024, doi: 10.1109/ACCESS.2023.3349091.
- [6] Shees, M. A. Taher and A. Sarwat, "Performance Analysis of ANSI C12.22 Protocol for Secure Smart Meter Communication in Advanced Metering Infrastructure," in *IEEE Open Journal of the Industrial Electronics Society*, vol. 6, pp. 1831-1847, 2025, doi: 10.1109/OJIES.2025.3628566.
- [7] T. Thambiran, M. Batool, Y. Fan, N. Zanib and F. Nawaz, "Upgradation of Metering Infrastructure of Low Voltage Distributed Network in Nottingham Road, Kwa-Zulu Natal, South Africa," in *IEEE Access*, vol. 12, pp. 22687-22706, 2024, doi: 10.1109/ACCESS.2023.3335659.
- [8] M. U. Saleem, M. R. Usman, M. A. Yaqub, A. Liotta and A. Asim, "Smarter Grid in the 5G Era: Integrating the Internet of Things with a Cyber-Physical System," in *IEEE Access*, vol. 12, pp. 34002-34018, 2024, doi: 10.1109/ACCESS.2024.3372379.
- [9] N. Bawankar, A. Kriti, S. S. Chouhan and S. Chaudhari, "IoT-Enabled Water Monitoring in Smart Cities With Retrofit and Solar-Based Energy Harvesting," in *IEEE Access*, vol. 12, pp. 58222-58238, 2024, doi: 10.1109/ACCESS.2024.3392852.
- [10] K. Srisomboon, K. Wasayangkool and W. Lee, "Trilateral Smart Switching Algorithm for Improving Smart Meters Efficiency in Advanced Metering Infrastructure (AMI) Network," in *IEEE Access*, vol. 12, pp. 194973-194988, 2024, doi: 10.1109/ACCESS.2024.3520601.
- [11] H. Kumar, O. A. Alvarez and S. Kumar, "Experimental Evaluation of Smart Electric Meters' Resilience Under Cyber Security Attacks," in *IEEE Access*, vol. 11, pp. 55349-55360, 2023, doi: 10.1109/ACCESS.2023.3278738.
- [12] P. Biswas *et al.*, "An Extensive and Methodical Review of Smart Grids for Sustainable Energy Management-Addressing Challenges with AI, Renewable Energy Integration and Leading-edge Technologies," in *IEEE Access*, doi: 10.1109/ACCESS.2025.3537651.
- [13] J. Huang, Y. Zhu, L. Xu, Z. Zheng, W. Cui and M. Sun, "On-Device Training of PV Power Forecasting Models in a Smart Meter for Grid Edge Intelligence," in *IEEE Open Access Journal of Power and Energy*, doi: 10.1109/OAJPE.2026.3657191.
- [14] Y. Santo, A. Abelém, A. Riker and E. E. Tsiropoulou, "Integrating Data Privacy and Energy Management in Smart Cities With Partial Sustainable IoT Networks," in *IEEE Access*, vol. 13, pp. 33176-33188, 2025, doi: 10.1109/ACCESS.2025.3541213.
- [15] F. B. B. Rolim, F. C. L. Trindade and V. C. Cunha, "Composite Index for Identifying Anomalies in Low Voltage Systems Using Smart Meter Measurement Data," in *IEEE Open Access Journal of Power and Energy*, vol. 12, pp. 306-317, 2025, doi: 10.1109/OAJPE.2025.3570834.