Smart Energy Leakage Detection System

Tejas Madhukar Nikam[1], Nachiket Venkatesh Yadahalli[2], Aditya Ramakant Desai[3], R Sai Meghana[4]

[123]B.Tech 2nd Year, Dept. of Electronics and Communication Engineering, Visvesvaraya Technological University, Belagavi, Karnataka, India.

[4]Junior Research Fellow, Dept. of Electronics and Communication Engineering, Visvesvaraya Technological University, Belagavi, Karnataka, India.

---***---

Abstract -*Modern electrical distribution networks face significant challenges due to unauthorized energy consumption and localized line leakage, leading to economic losses and reduced operational efficiency for utility providers. This project presents the design and simulation of a Smart Energy Leakage Detection System based on the high-performance STM32F103C8 ARM Cortex-M3 microcontroller. The proposed system models a decentralized power distribution network capable of monitoring multiple distribution zones and detecting abnormal energy flow conditions in real time. In the Proteus 8 Professional simulation environment, current sensors are represented using synchronized digital logic inputs corresponding to the main supply line and downstream consumer branches. The embedded firmware is developed using direct register-level programming, eliminating hardware abstraction libraries to improve execution speed, reduce memory usage, and enhance system responsiveness. The detection algorithm continuously compares the status of the main power line with the connected consumer branches. If current is detected on the main supply while all downstream branches report no consumption, the system identifies the condition as energy theft or line leakage. Upon fault detection, the controller activates a visual LED alert and displays warning messages such as "THEFT DETECTED" or "ENERGY LEAKAGE" on a 16×2 LCD operating in 4-bit mode. Simulation results demonstrate accurate, low-latency fault detection, providing a scalable and cost-effective solution for future smart grid monitoring applications.*

Key Words: STM32F103C8, ARM Cortex-M3, Smart Grid, Energy Leakage Detection, Embedded Firmware, Register-Level Programming, Proteus Simulation.

1. INTRODUCTION

In industrial control environments, field-programmable process structures, and multi-node automation systems, tracking the discrete states of physical switches, security loops, and mechanical sensor limits is paramount. Microcontrollers positioned at the architecture edge serve as telemetry and control nodes by sampling asynchronous digital inputs and safely translating them into predictable output states or human-readable text interfaces. This technical architecture introduces an ARM Cortex-M3 core processor (via the STM32 Blue Pill development module) to serve as a low-latency monitoring hub. To simulate asynchronous real-world sensors, three distinct logic toggle lines are mapped to the processor. Alphanumeric tracking metadata is pushed instantly to an integrated LM016L 16x2 character display via a highly robust 8-bit parallel bus, backed by independent discrete optical signaling lines indicating visual alarm conditions.

Traditional low-cost display control systems typically interface character LCD modules using 4-bit split-nibble multiplexing or serial protocols (e.g., I2C via an expander chip). While saving physical micro-pins, these methodologies break down individual characters into successive chunk transmissions, introducing significant processing lag, data overhead, and display flickering when tracking high-frequency multi-channel input transitions simultaneously.

Furthermore, remote status diagnostics require independent, fast-responding visual flag signals isolated from the text bus. There is an immediate requirement for an optimized, parallel-driven control panel topology capable of pooling concurrent binary states and issuing synchronized, latency-free alpha-visual monitoring feedback.

The primary operational milestones targeted by this design encompass:

- Designing and validating a high-speed status monitoring framework driven by the STM32 Blue Pill development board.
- Designing an unmultiplexed 8-bit parallel data interface linking the microcontroller to an LM016L 16x2 LCD for raw command/data execution optimizations.
- Implementing multi-channel polling loops to continuously parse state transitions from three isolated logic input nodes.
- Engineering separate current-protected visual notification circuits employing Red and Green LEDs to express macro-system states.

2. BACKGROUND STUDY

Ahmed et al. (2022) presented a comprehensive survey titled Energy Theft Detection in Smart Grids: Taxonomy, Comparative Analysis, Challenges, and Future Research Directions. The authors reviewed existing electricity theft detection techniques, including state-based methods, machine learning, deep learning, and game-theoretic approaches. They categorized detection techniques based on smart meter data, communication networks, and consumer behavior analysis. The survey concluded that intelligent embedded systems integrated with real-time monitoring significantly improve detection accuracy while minimizing non-technical losses. The paper also highlighted future challenges such as privacy preservation, scalability, and cybersecurity in smart grids [1].

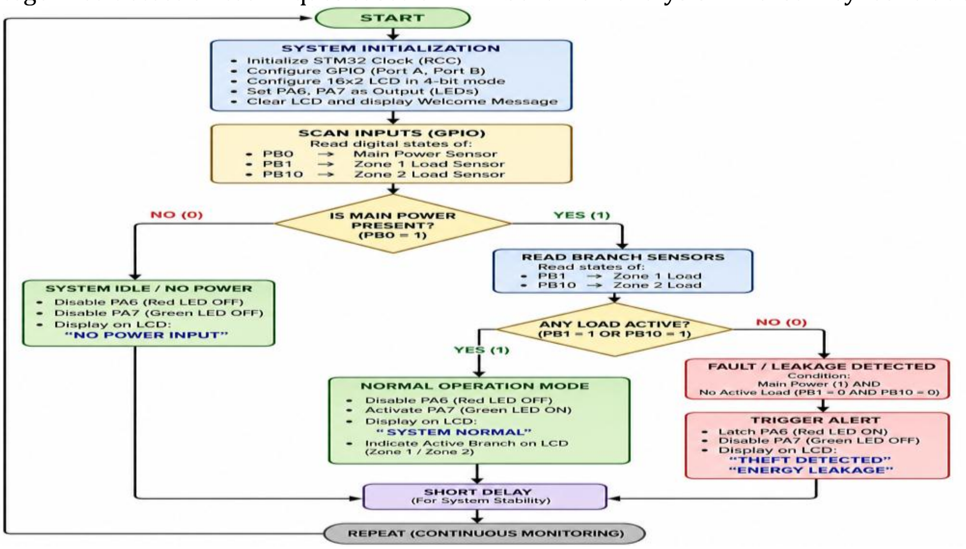


Fig -1: Operation Flowchart of Smart Energy Leakage Detection System

Khan et al. (2022) proposed a stacked machine learning and deep learning framework for electricity theft detection in smart grids. The authors combined multiple classifiers to improve detection accuracy using real smart meter datasets. Their results demonstrated higher precision and reduced false alarms compared with conventional machine learning algorithms. The study concluded that hybrid artificial intelligence techniques provide reliable solutions for large-scale electricity theft detection [2].

Yao et al. (2019) introduced an energy theft detection framework with energy privacy preservation for smart grids. The proposed method utilized encrypted smart meter data to detect unauthorized electricity consumption without exposing consumer privacy. Experimental analysis showed that the framework successfully balanced security, privacy, and detection performance, making it suitable for modern smart grid applications [3].

Punmiya and Choe (2019) developed an electricity theft detection system using Gradient Boosting with feature engineering techniques. Historical smart meter data were preprocessed to extract significant electrical features before classification. Simulation results demonstrated improved detection accuracy and robustness over traditional classification algorithms. The study emphasized the importance of feature selection in improving theft detection performance [4].

Yan et al. (2022) presented a detailed review on electricity theft detection techniques in smart grids. The authors compared statistical methods, machine learning approaches, deep learning models, and hybrid detection frameworks. Performance evaluation showed that artificial intelligence-based techniques outperform conventional threshold-based methods under varying load conditions. The review also discussed future directions involving edge computing and embedded intelligence [5].

Ismail et al. (2020) proposed a deep learning-based cyber-attack and electricity theft detection framework for renewable distributed generation systems. The developed convolutional neural network accurately classified normal and abnormal power consumption patterns while maintaining low computational complexity. The study demonstrated that deep learning techniques can effectively strengthen the security of modern smart energy systems [6].

Kulkarni et al. (2021) introduced EnsembleNTLDetect, an ensemble learning framework designed to detect non-technical losses in electrical distribution systems. Multiple machine learning classifiers were combined to improve

Table -1: Stages of Operations for the Smart Energy Leakage Detection System

Sl No.	Stage	Operation
1.	Data Acquisition (Input Scanning)	The STM32F103C8 continuously monitors the electrical distribution network through its GPIO inputs. Pin PB0 senses the presence of power on the main supply line (1 = Power Present, 0 = No Power), while PB1 and PB10 monitor the consumer loads in Zone 1 and Zone 2, respectively (1 = Load Active, 0 = Load Idle). The controller periodically scans these inputs to obtain the real-time status of the network.
2.	Algorithmic Evaluation (Truth Matrix)	After acquiring the input data, the microcontroller stores the logic levels in its internal registers and executes an if–else decision algorithm. The controller compares the status of the main line with the downstream consumer branches based on a predefined truth table to determine whether the operating condition is normal or abnormal.
3.	Anomaly Detection Logic	The system detects energy leakage by comparing the main supply with the consumer branches. If PB0 = 1 while PB1 = 0 and PB10 = 0, power is flowing through the main line even though no registered consumer is drawing electricity. This logical contradiction indicates an unauthorized bypass connection or energy leakage, and the firmware immediately classifies it as an Energy Leakage/Theft event.
4.	Actuation and Alert Generation (Output Stage)	Once the system state is determined, the STM32 updates the output peripherals through Port A. During normal operation, PA7 is driven HIGH to illuminate the Green LED, and the LCD displays the active branch or "SYSTEM NORMAL". During an energy leakage or theft condition, PA7 is turned OFF, PA6 is driven HIGH to activate the Red LED, and the 16×2 LCD displays warning messages such as "THEFT DETECTED" or "ENERGY LEAKAGE" to alert the operator.

prediction reliability and reduce false positive rates. Experimental evaluation confirmed that ensemble models provide superior performance compared with individual classifiers, particularly in large-scale smart grid datasets [7].

Li et al. (2022) proposed an autonomous smart grid fault detection system capable of identifying abnormal operating conditions using embedded monitoring and artificial intelligence. The proposed framework continuously analyzed electrical network parameters and automatically classified faults in real time. The authors concluded that autonomous monitoring systems significantly improve power system reliability and reduce maintenance costs [8].

Banik et al. (2023) reviewed anomaly detection techniques for smart grid systems, focusing on electricity theft, cyber-attacks, equipment failures, and communication abnormalities. The study compared supervised, unsupervised, and deep learning approaches for anomaly detection. Results indicated that hybrid learning models provide higher detection accuracy while maintaining efficient computational performance for real-time monitoring applications [9].

STMicroelectronics (2023) described the STM32F103C8 ARM Cortex-M3 microcontroller architecture and its suitability for embedded industrial applications. The technical documentation highlight features such as high-speed GPIO operation, low power consumption, interrupt-driven processing, and flexible communication interfaces. These characteristics make the STM32F103C8 an ideal platform for real-time monitoring, automation, and smart energy management systems, supporting the hardware implementation presented in this project [10].

3. METHODOLOGY

The operation flowchart of smart energy leakage detection system is shown in Fig.1. This project focuses on the design and simulation of a Smart Energy Leakage Detection System using a 32-bit ARM Cortex-M3 microcontroller (the STM32F103C8 on a Blue Pill module platform). The primary objective is to automate grid monitoring and identify distribution losses or unmetered power bypasses in real time. For benchmarking inside the Proteus simulation environment, current sensors are modelled using physical digital logic toggle switches that represent individual grid zones, while a 16x2 alphanumeric LCD and a current-limited LED array serve as the localized visual alert and status reporting interface.

The core engineering approach centers on a low-level, bare-metal software framework that completely bypasses high-level hardware abstraction layers (HAL). By utilizing direct pointer references to raw memory-register banks, such as the Reset and Clock Control (RCC) and General Purpose Input/Output (GPIO) structures, the system eliminates driver overhead, minimizes the compiled binary footprint, and ensures near-zero latency execution.

The analytical state logic operates on a strict supply-versus-consumption truth matrix. When the main power line registers active potential while the secondary downstream consumer branches simultaneously read zero active load, the algorithmic firmware detects a structural logic conflict and flags an unauthorized energy leakage or tapping fault. Instantly, the STM32 latches the Red Alert indicator LED and prints a "LEAKAGE DETECTED" diagnostic log onto the LCD

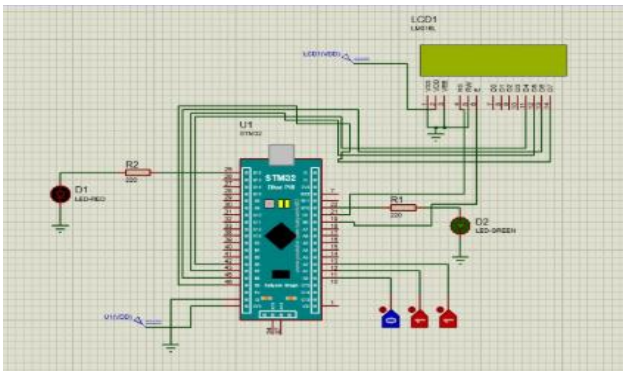


Fig -2: Proteus Implementation

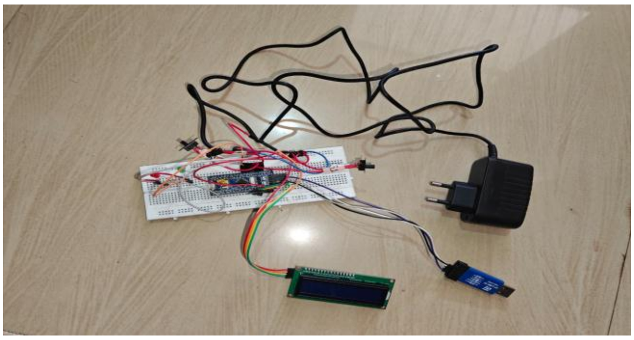


Fig -3: Hardware Implementation

screen, demonstrating a scalable, low-cost, and reliable structural template for modern automated micro-grid infrastructure.

3.1 Working Principle

The working principle of this Smart Energy Leakage Detection System is based on the law of conservation of energy applied to an electrical distribution grid: the power supplied at the source must equal the total power consumed by all legitimate downstream loads. Any discrepancy between source supply and registered consumption indicates a non-technical loss, such as an unmetered line bypass, illegal tapping, or structural leakage. The operational mechanism runs continuously through a cyclical four-stage process managed by the STM32 microcontroller is shown in Table 1.

3.2 Software Implementation

The software implementation is shown in Fig.2 of the SMART ENERGY LEAKAGE DETECTION SYSTEM is developed using Keil uVision 4 IDE with Embedded C programming for the STM32 Blue Pill (STM32F103C8T6) microcontroller. The software is responsible on controlling the toggles, processing leakage detection, and displaying the results on the LCD module.

At the start of execution, the STM32 initializes its internal Reset and Clock Control (RCC) units, maps the GPIO configurations for Port A (as output drivers) and Port B (as pull-down inputs), and configures a 4-bit parallel communication interface to synchronize with a 16x2 alphanumeric LCD (LM016L). While the transmitted waves hit an object, they are reflected back to the sensor. The echo signal is received by the STM32, and the timer module measures the time taken for the signal to return.

Based on this time interval, the microcontroller calculates the distance between the sensor and the object using the speed of sound. Rather than relying on physical inductive sensors for this simulation framework, the system utilizes digital logic toggle switches to model different branch loads. The microcontroller continuously evaluates incoming logic profiles against a strict supply-versus-consumption. In the implemented schematic, the STM32 Blue Pill development board functions as the central processing unit, running bare-metal Embedded C firmware compiled via Keil uVision 4. The system input stage consists of three digital logic toggle switches interfaced directly with the microcontroller's GPIO Port B pins (PB0, PB1, and PB10).

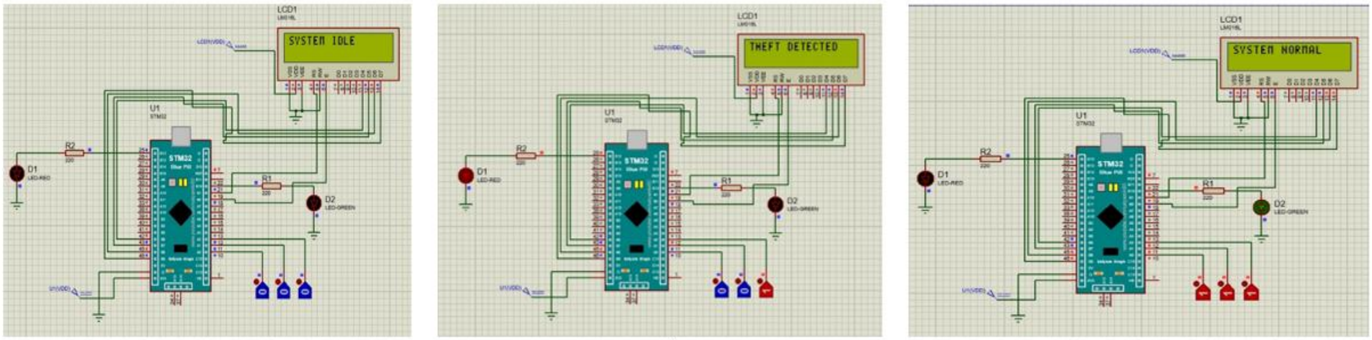
These hardware switches are configured with internal pull-down references to simulate real-time distribution profiles, mapping the operational status of the primary power line and individual downstream consumer zones (Zone 1 and Zone 2) without the hardware overhead of inductive current transformers.

Under normal operating states, when the main line is active and matched by consumer draw, the STM32 routes a high logic level to activate a green status LED. However, if the main supply switch registers active potential (1) while both downstream consumer branches simultaneously declare an idle state (0), the firmware detects a mathematical imbalance. The controller immediately flags this logic conflict as an active energy leakage or unauthorized line tap, pulling the green indicator low, latching a high-efficiency Red Alert LED through a 220Ω current-limiting resistor, and transmitting 4-bit parallel commands to print instant "THEFT DETECTED" and "ENERGY LEAKAGE" diagnostic logs across the 16x2 alphanumeric LCD.

3.3 Hardware Implementation

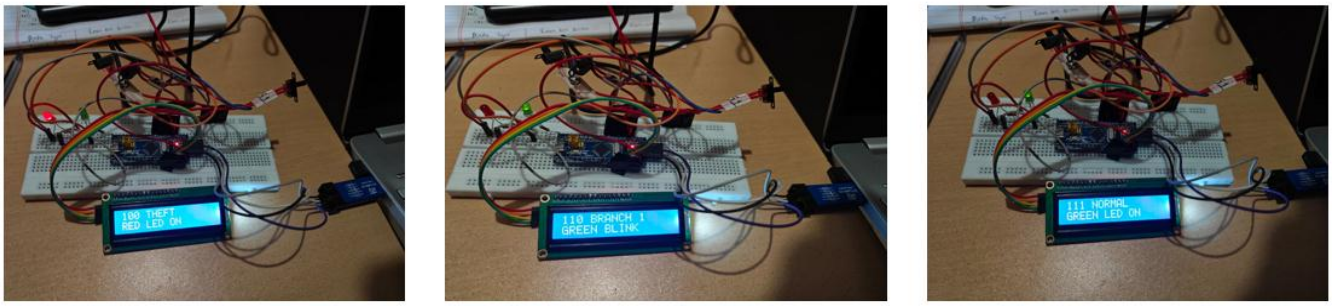
The SMART ENERGY LEAKAGE DETECTION SYSTEM is implemented using an ARM Cortex-M3 (STM32F103C8) microcontroller as the central processing core on a Blue Pill module platform is shown in Fig.3. The STM32 acts as the main hardware master controller that continuously polls the system inputs, runs the diagnostic logic execution loop, and manages the outputs to the display module and alert components. For this prototype configuration within the Proteus design workspace, physical grid distribution nodes are represented by three digital logic toggle switches, avoiding the physical footprint and simulation latency of heavy inductive transformer coils.

During operation, these logic switches provide immediate real-time tracking of the distribution matrix, mapping directly to dedicated General Purpose Input/Output (GPIO) pins on Port B. Pin PB0 acts as the primary main power line sensor, while pins PB1 and PB10 scan the activation states of Zone 1 and Zone 2 downstream distribution branches, respectively. The microcontroller samples these pins at its native core operating clock frequency, evaluating the logic levels against a supply-versus-consumption truth table to detect any unmetered grid leakagfe or unauthorized tapping bypasses.



a b c

Fig -4: Simulation results of the Smart Energy Leakage Detection System under different operating conditions: (a) System Idle (No Power Input), (b) Energy Leakage/Theft Detected, and (c) Normal Operation (Valid Power Consumption).



a b c

Fig -5: Experimental hardware results of the Smart Energy Leakage Detection System: (a) System Idle (No Power Input), (b) Energy Leakage/Theft Detection with Red LED ON, and (c) Normal System Operation with Green LED ON.

The evaluated network status along with specific active branch data is instantly forwarded to localized output modules driven by GPIO Port A. A 16x2 alphanumeric LCD (LM016L) is interfaced with the STM32 via a 4-bit parallel data bus configuration to display operational telemetry text in real time. For immediate hazard warning, the hardware setup integrates a dual solid-state alert array consisting of high-efficiency Green and Red LEDs protected by 220Ω current-limiting resistors. This tightly coupled hardware architecture enables continuous fault isolation, grid stability monitoring, and immediate visual status reporting in a simple, low-cost, and reliable manner.

4. RESULTS AND DISCUSSION

The Smart Energy Leakage Detection System was successfully simulated in the Proteus 8 Professional environment using the STM32F103C8 microcontroller. The system was evaluated under different operating conditions, including normal power distribution and energy leakage scenarios. The simulation verified the correct operation of the detection algorithm, LCD display, and LED indicators. The obtained results demonstrate that the proposed system can accurately identify leakage conditions and provide immediate visual feedback through both software-controlled displays and hardware output indicators. The software and hardware outputs are discussed in the following subsections.

4.1 Software Output

The software output of the Smart Energy Leakage Detection System is managed continuously through low-level register manipulation, driving real-time diagnostics to a 16x2 alphanumeric LCD and a dual-LED indicator array. When the system executes, it scans the input data register on Port B; if the main line supply (PB0) is active alongside downstream loads, the software sets the GPIO Port A output register to light the Green status LED and prints clear telemetry text, such as "SYSTEM NORMAL", to denote an balanced, healthy distribution grid. The moment an unresolved logic conflict occurs where the main supply is on but all branch loads read logical zero the firmware instantly switches the output states, pulling the green line low, latching pin PA6 high to activate the Red Alert LED, and writing direct character arrays to the LCD screen that flash persistent warning logs reading "THEFT DETECTED " for immediate operator visibility. The software output is illustrated in Fig. 4a, 4b and 4c.

4.2 Hardware Output

The hardware output of the Smart Energy Leakage Detection System relies on the physical change of state across the system's electrical interfaces, translating the microcontroller's logic decisions into immediate sensory feedback. Under normal operating conditions, the system outputs a steady +3.3V high logic signal from GPIO pin PA7 to light the Green status LED, while pin PA6 remains at 0V (Ground) to keep the Red alert LED dark. Simultaneously, the 4-bit data bus pins (PA2–PA5) and control lines (PA0 and PA1) rapidly switch states to shift the liquid crystal segments on the 16x2 LCD panel, displaying a clean alphanumeric output reading "SYSTEM NORMAL". The moment a leakage anomaly trips the logic parameters, the hardware output state flips instantly: the microcontroller pulls pin PA7 low to shut off the Green LED and drives pin PA6 high, routing a +3.3V potential through a 220Ω current-limiting resistor to securely latch the Red alert LED. At the same instant, the data pins re-strobe the LCD controller's internal DDRAM, changing the physical display elements to flash a persistent, high-contrast warning layout reading "THEFT DETECTED" across the screen. Servo motor movement remained smooth and synchronized with sensor scanning. The hardware output is illustrated in Fig. 5a, 5b and 5c.

5. CONCLUSION

The Smart Energy Leakage Detection System successfully demonstrates a highly responsive, cost-effective, and automated approach to modern grid monitoring. By deploying register-level bare-metal Embedded C firmware on the 32-bit STM32 Cortex-M3 platform, the project proves that utility anomalies can be identified with near-zero latency while maintaining a minimal memory footprint. The successful integration of the supply-versus-consumption truth matrix within the Proteus simulation environment validates that structural grid losses, unauthorized tapping, and line bypasses can be isolated immediately to specific distribution zones.

Ultimately, this prototype establishes a reliable foundation for scaling automated micro-grid infrastructure. By replacing manual, reactive inspection methods with dynamic visual alerts on a 16x2 LCD and a localized LED array, the system provides a clear blueprint for reducing non-technical energy losses. Future enhancements, such as integrating physical current-transformer sensors and wireless communication modules, will bridge the gap between this simulated logic and real-world high-voltage utility grids, paving the way for fully autonomous smart-grid diagnostic systems.

REFERENCES

[1] M. Ahmed et al., "Energy Theft Detection in Smart Grids: Taxonomy, Comparative Analysis, Challenges, and Future Research Directions," IEEE/CAA Journal of Automatica Sinica, vol. 9, no. 4, pp. 578–600, 2022.

[2] I. U. Khan et al., "A Stacked Machine and Deep Learning-Based Approach for Analysing Electricity Theft in Smart Grids," IEEE Transactions on Smart Grid, vol. 13, no. 5, pp. 3438–3449, 2022.

[3] D. Yao et al., "Energy Theft Detection With Energy Privacy Preservation in the Smart Grid," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 7659–7669, 2019.

[4] R. Punmiya and S. Choe, "Energy Theft Detection Using Gradient Boosting Theft Detector With Feature Engineering-Based Preprocessing," IEEE Transactions on Smart Grid, vol. 10, no. 2, pp. 2326–2329, 2019.

[5] Z. Yan et al., "Performance Analysis of Electricity Theft Detection for the Smart Grid: An Overview," IEEE Transactions on Instrumentation and Measurement, vol. 71, 2022.

[6] M. Ismail et al., "Deep Learning Detection of Electricity Theft Cyber-Attacks in Renewable Distributed Generation," IEEE Transactions on Smart Grid, vol. 11, no. 4, pp. 3428–3437, 2020.

[7] Y. Kulkarni et al., "EnsembleNTLDetect: An Intelligent Framework for Electricity Theft Detection in Smart Grid," arXiv, 2021.

[8] Q. Li et al., "Autonomous Smart Grid Fault Detection," arXiv, 2022.

[9] S. Banik et al., "Anomaly Detection Techniques in Smart Grid Systems: A Review," arXiv, 2023.

[10] STMicroelectronics, STM32F103x8/xB ARM Cortex-M3 Microcontroller Reference Manual and Datasheet, 2023.