# System for Detecting and Preventing Energy Theft

Hussain Kassim Ahma
Al-Rafidain University College
Baghdad, Iraq
hussain.shtb@ruc.edu.iq

Sahar Ali Abdulkareem
Al-Turath University College
Baghdad, Iraq
sarah.ali@turath.edu.iq

Alaa Salim Abdalrazzaq
Al-Noor University College
Nineveh, Iraq
alaa.salim@alnoor.edu.iq

Mariia Liashchenko
Kyiv National University of
Construction and Architecture,
Kyiv, Ukraine
liashchenko_ma@knuba.edu.ua

***Abstract*—Background: Energy theft in developing nations reduces electricity quality and availability for legal consumers and costs energy suppliers much money. Poor power distribution network maintenance and management compound these nations' energy supply issues.**

**Objective: This study will design, develop, and deploy a monitoring and deterrence system for power grid theft. The approach reduces revenue losses for energy providers and improves electricity quality for legitimate users, improving power infrastructure health.**

**Methods: Sensors, communicators, and software algorithms comprise the proposed system. These sensors monitor current and voltage, detect power line tapping attempts, and identify irregular consumption patterns that may indicate energy theft. Software algorithms evaluate sensor data and notify authorities of suspected thefts when these abnormalities are detected.**

**Results: Energy providers should expect lower revenue losses and better power quality for legitimate customers using the system. The technique may also reduce power infrastructure pressure and equipment failures from theft overloads.**

**Conclusion: A robust grid power theft monitoring and prevention system is feasible and essential. Energy suppliers will profit, while genuine consumers will get better power and fewer interruptions. Implementing the entire system offers a reliable, high-quality electrical supply for everybody.**

## I. Introduction

Energy is a fundamental resource for economic growth and development in any country. It is a crucial component of modern life, and its availability is essential for the smooth functioning of transportation and daily life activities. Despite being an essential commodity, energy theft is a persistent problem in developing countries, resulting in significant revenue losses for energy providers and negatively impacting the quality and availability of power for legal users. Electricity theft is considered a crime in most countries and can lead to legal action against the offenders [1].

Energy theft refers to any unauthorized use of electricity not recorded or paid for by the user. It can take various forms, such as meter tampering, bypassing, or directly tapping the power lines. Energy theft is a significant challenge in developing countries. The power distribution network is often poorly maintained and managed, making it easier for offenders to commit theft without detection [2].

The impact of energy theft on developing countries' economies is significant. It results in revenue losses for energy providers, reducing the funds available for maintenance and expansion of the power distribution network [3]. This, in turn, negatively affects the quality and availability of power for legal users, leading to further losses in revenue for businesses that rely on a continuous and reliable supply of electricity.

The article aims to design and implement a system for detecting and preventing energy theft in the power distribution network. The system consists of sensors, communication devices, and software algorithms that monitor energy consumption patterns and detect anomalies that suggest theft [4]. These sensors detect attempts to tap power directly from the lines, monitor voltage and current levels, and identify unusual usage patterns that could indicate energy theft. The software algorithms analyze the data collected by these sensors and generate alerts to the authorities in case of any potential theft in the area [5].

The ultimate goal of this research is to ensure that everyone has access to continuous, high-quality power, and the system's implementation can go a long way in achieving this goal. By detecting and preventing energy theft, this system can help reduce energy providers' revenue loss and improve the quality of power supplied to legal users. The system's implementation can also help reduce the burden on the power distribution network and prevent equipment failures caused by overloading [6].

In conclusion, energy theft is a significant challenge in developing countries, and it negatively impacts the economy, quality of life, and the environment. Implementing a system for detecting and preventing energy theft can go a long way in addressing this issue, ensuring everyone has access to continuous and high-quality power and reducing the burden on the power distribution network. This research demonstrates the feasibility of designing and implementing an effective system for detecting and preventing energy theft in the power distribution network, which can help improve the quality of

power supplied to legal users, reduce equipment failures, and prevent revenue losses for energy providers.

### *A. Problem Statement*

Theft of energy is a recurrent issue in developing nations. This is because the electricity distribution network in these countries needs to be better managed, making it more straightforward for thieves to steal energy without being caught. The theft of energy has a substantial negative influence on the economies of developing nations because it causes lost revenues for energy suppliers, which reduces the amount of money that can be used for the maintenance and growth of the electricity distribution system. This, in turn, has a detrimental effect on the quality and accessibility to electricity for legitimate users, which leads to further income losses for enterprises that depend on a consistent and dependable supply of energy. Theft of energy is a widespread problem in developing nations, even though it is a criminal offence; hence, there is a pressing want for an efficient way to solve this obstacle. As a result, the problem definition for this article is to create and put in place a mechanism to identify and try to prevent energy theft in the network that distributes electricity. This system can assist in improving the quality of the energy provided to legal users, reduce equipment failures, and prevent economic damage for energy providers.

### *B. The Aim of the Article*

This article aims to solve the problem of energy theft in developing nations by establishing a mechanism for identifying and stopping energy robbery in the power distribution network. That will be accomplished by tackling the problem of energy theft in emerging regions. This article aims to draw attention to the adverse effects that illegally obtaining energy may have on the economies of developing nations, the life expectancy of legitimate users, and the ecology. In addition, the purpose of this article is to demonstrate that it is possible to design and implement an efficient system for detecting and preventing the theft of energy, as well as the potential of such a system to improve the quality of the power supplied to legal users, reduce the number of equipment failures, and prevent revenue losses for energy providers. Ultimately, this study aims to contribute to the current discourse on energy theft in developing nations and suggest a possible solution to this ongoing problem.

## II. LITERATURE REVIEW

Energy theft is a big issue for power companies, which results in significant revenue losses and increasing prices for end users. With the research that has been done on this issue, some different solutions have been suggested.

The article by Qi et al. gives an overview of the problem of energy theft, including its causes and implications on the power system. The authors offer a strategy for controlling theft based on using intelligent meters. This technique incorporates the use of real-time data from smart meters in order to detect theft and identify the location of the crime [7].

The authors Bebonchu Atems and Chelsea Hotaling [8] explore the economic effects of technical and non-technical losses in the electricity system, specifically in India's economy. The authors contend that lowering losses may result in substantial cost savings for end users and thus contribute to an increase in the competitiveness of the power industry from a monetary standpoint.

A framework for detecting energy theft using several sensors is proposed by Singh et al. [9] for use in advanced metering networks. The system detects and localizes theft using several sensors and combines machine learning techniques to increase detection accuracy.

Yao et al. [10] examine the issues involved with the intelligent grid regarding security and privacy, including the possibility of energy theft. The authors contend that to overcome these difficulties, new regulations and technology about security and privacy will need to be developed.

The knowledge-based approach for non-technical loss detection that Jeanne Pereira and Filipe Saraiva [11] propose combines statistical methods, text mining, and neural networks to identify potential better problems. The technology analyzes data from the past to recognize patterns of anomalous behaviour and locate possible instances of theft.

The authors of Hussain et al. [12] provide a new method for feature selection that uses harmony search and demonstrates how it may be used to detect non-technical loss. The essential elements from the collected data are extracted by the algorithm so that it may utilize them to educate a classifier.

Prakash et al. [13] comprehensively review artificial intelligence methodologies and non-technical loss detection. The authors emphasize the problems and possibilities associated with these approaches and address the possibility of their integration into current power systems. They also discuss the potential for these techniques to be integrated into existing power systems [14].

Using state estimation and analysis of variance, Yuanqi Gao et al. [15] describe a technique for detecting losses that do not need technical expertise. The approach utilizes the data from smart meters to estimate the amount of energy used by individual customers and to identify any irregularities that may indicate theft.

In their study, Leite and Mantovani [16]describe a technique for identifying and localizing non-technical losses in contemporary distribution networks. This -learning approach recognizes anomalous behaviour patterns and pinpoints possible theft instances.

Zheng et al. [17] propose an extensive and deep convolutional neural network to identify instances of power theft. The network employs deep and shallow layers to extract pertinent aspects from the data and categorize consumers as authentic or prospective crooks.

In general, the examination of the relevant literature demonstrates how important it is to create efficient systems for detecting and preventing energy theft inside the power system. There is a wide range of complexity and efficiency in the many ways that have been suggested. Further study is required to identify which approaches will be the most useful for various power systems and consumer profiles.

## III. METHODOLOGY

Power companies all over the globe have to deal with the problem of energy loss throughout electricity transmission and

distribution. This problem may be categorized into technical losses (TLs) and non-technical losses (NTLs). Internal actions in power system components such as transformers cause TLs. In contrast, NTLs are primarily caused by electricity theft through physical attacks such as tapping lines, breaking meters, or tampering with meter readings [18]. External factors, such as lightning, can also cause TLs. Theft of electricity leads to a loss of income for power providers, which is estimated to be over $4.5 billion yearly in the United States, and it may also represent a concern for the public's safety owing to the excessive strain that is placed on electrical systems, which can cause fires. Because of this, reliable detection of energy theft is essential for ensuring the safety and stability of power grids [19], [20].

Advanced metering infrastructure, often known as AMI, is a component of smart grids that enables power companies to get enormous volumes of data on energy use from smart meters at a high frequency. This data may assist in the detection of electricity theft [21]. However, since it uses digital tools and can be attacked digitally, the AMI network makes it easier for criminals to steal electricity and commit cybercrime. Human inspection of unlawful line diversions, comparison of malicious and benign meter data, and evaluation of malfunctioning equipment or hardware are now the critical approaches for detecting power theft [7]. Nevertheless, these manual procedures require much time and resources and cannot thwart cyberattacks.

Several models, such as those based on state logic, game theory, and artificial intelligence, have been presented by authors as potential solutions to the problem of energy theft. These models are intended to combat the problems that have been identified. State-based detection depends on specialized equipment such as wireless sensors and distribution transformers [22]. However, it also needs the real-time capture of system topology and extra physical measurements, which may not be possible. Game-based detection works by simulating a competition between an electricity provider and a potential thief to derive distributions of normal and aberrant behaviours from the game's equilibrium [23]. Nevertheless, determining how each player's utility function should be calculated remains a difficult task.

Methods based on artificial intelligence have also been suggested [16], [24], [25]. These approaches include machine learning and deep learning techniques. Nevertheless, the present techniques of machine learning detection still have a limited capacity to deal with high-dimensional data and need the human extraction of features, which is a procedure that is both laborious and time-consuming. Convolutional neural networks (CNNs), long-short-term memory (LSTM), recurrent neural networks (RNNs), and stacking autoencoders are some of the deep learning approaches that have been examined [26]. Nevertheless, the performance of the detectors was evaluated using simulated data. The article [27] suggests a deep neural network (DNN)--base customer-specific detector as an effective countermeasure against cyberattacks. CNN has seen widespread use in extracting characteristics for power theft detection from high-resolution smart meter data [20].

### *A. Description*

We designed the current project based on the overload that is above the average load on the house or any other place, depending on the value that we put inside the programmingin the Arduino through the line ( if(( currentAcc >= 2500) && (flag1 == 1)) ). We get this reading by reading the current sensor (ACS712 current sensor) and showing the result in the ( serial monitor ) of the Arduino. From here, we can determine the value of the load for the house after operating several home appliances to follow the change that occurs in the ( serial monitor ) for Arduino. Then we put this value in the programming and carry it on the Arduino, but on the condition that the value of carrying the current of the current sensor must be taken into account because there are many values for it, such as 5 volts, 10 volts, 30 volts. There are also many types when searching on the Internet.

Usually, when there is no load or theft on the current, the system worksand the LCD shows an average load.


Fig. 1. Normal load

Moreover, the system usually works when one lamp is turned on because the load is average, and the LCD shows a normal load.

Moreover, when two lights are turned on, the system will give an audible alert to indicate an overload on the system, and the LCD will show the presence of theft of the load.


Fig. 2. Overload load

### *B. Hardware Requirement*

The hardware requirements will depend on the specific design and implementation of the system. However, here are some essential hardware components that may be required:

- Arduino [28] board will serve as the system's central processing unit (CPU). The specific model of the Arduino board will depend on the complexity of the system and the number of sensors and actuators that

will be used.

- Sensors [29]: The system will require various sensors to detect energy theft. These may include current sensors, voltage sensors, and power sensors. The number and type of sensors will depend on the system's specific requirements.
- Actuators: The system may require actuators, such as relays or switches, to prevent energy theft and turn off power to a specific location when energy theft is detected.
- Communication module: The system will require a communication module to send alerts and data to a central monitoring system. This may be a Wi-Fi or GSM [30] module.
- Power supply: The system will require a power supply to power the Arduino board [31]and other components.
- Enclosure: The system may require an enclosure to protect the components from environmental factors and ensure safe operation.

Overall, the hardware requirements for a System for Detecting and Preventing Energy Theft will depend on the system's specific needs and the complexity level required.

*1) Arduino Uno (R3)*

The Arduino Uno (R3) is a popular microcontroller board designed for beginners and professionals. It is based on the ATmega328P [31] microcontroller and has a variety of input/output [32]pins that can be used for controlling and sensing different devices and signals.

The Arduino Uno (R3) board offers some features that make it an ideal choice for the construction of a system to detect and prevent the theft of energy, including the following:

There are 20 input/output pins on the Arduino Uno, which may be used to connect various sensors and other devices. Because of this, it is straightforward to interface with various components, such as current sensors, alarms, and relays.

The analogue-to-digital converter (ADC) on the Arduino Uno has 10 bits, which allows it to transform analogue signals from sensors into digital values that the microcontroller can utilize. This allows the analogue data to be handled by the microcontroller [33].

The Arduino IDE is a user-friendly software development environment that streamlines the process of developing code for the microcontroller, testing it, and uploading it to the microcontroller. It also allows the microcontroller to be programmed.

Since Arduino Uno is an open-source platform, all of its software, schematics, board layouts, and board designs are freely accessible to the general public. Because of this, it is elementary to adapt the platform to the requirements of individual applications [34].

The use of Arduino Uno in constructing a System for Identifying and Avoiding Energy Theft has the goals of monitoring energy consumption in real-time, identifying any irregularities or illegal usage, and taking preventative measures to stop energy theft [35]. Quickly connect with sensors and devices when using an Arduino Uno, collect and analyze data, and manage the power supply depending on the readings from the current sensor. All of these functions may be accomplished with ease. This has the potential to assist in lowering overall energy losses and enhancing the effectiveness of the energy distribution system.

*2) ACS712 for Energy Theft Prevention System*

Arduino may be part of a "System for Identifying and Preventing Energy Theft" to use the ACS712 current sensor, a popular kind of current sensor. It is a sensor based on the hall effect that can measure alternating and direct currents [36]. The following is a list of some of its properties, as well as some of the applications it may have:

Range of measurement: The ACS712 is offered in a few distinct iterations, each with a unique measuring range of either 5A, 20A, or 30A. Free to choose the variation for your application depending on the anticipated range of the current value.

The sensitivity of the ACS712 is 185 mV/A, which indicates that the sensor's output voltage will rise by 185 mV for each ampere of current that flows through it. In other words, the sensitivity of the sensor is relatively high.

Signal output: The ACS712 has an analogue output voltage proportional to the measured current. That is the signal that comes out of the device. With input currents ranging from -5A to +5A, the output voltage may vary from 0 to 5 volts [17]

Interface: To measure the output voltage and turn it into a digital value, the ACS712 may be linked to one of the analogue input pins on the Arduino Uno. This allows the user to connect it to the board.

You may connect the sensor to the power lines you wish to monitor to utilize the ACS712 in a "System for Monitoring and Preventing Energy Theft" using Arduino. This will allow you to detect and prevent energy theft. A burden resistor may be used to restrict the amount of current that flows through the sensor and transform the sensor's output voltage into a range that is detectable by the Arduino Uno. After everything is connected, you can read the output voltage from the ACS712 using one of the analogue input pins on the Arduino Uno and then use the inbuilt ADC [33] to convert it into a digital value. After that, use the digital value to compute the power consumption, discover any irregularities or illegal use, and take preventative measures to stop energy theft.

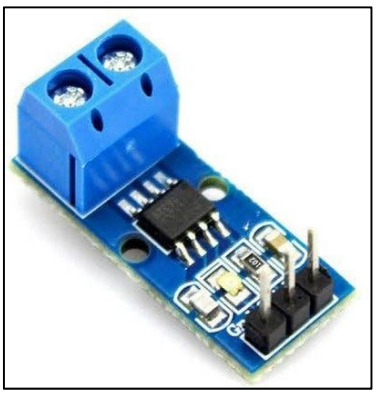

Fig. 3. LED Display Panel

The ACS712 current sensor can detect and prevent energy theft, a significant issue in many parts of the world. Here are the general steps to use the ACS712 current sensor for this purpose:

Install the ACS712 current sensor in the electrical circuit to monitor. That may involve cutting the circuit and inserting the sensor in series with the load or simply wrapping the conductor carrying the load with the sensor.

Connect the output of the ACS712 sensor to a microcontroller or other processing device that can process the signal and determine if the current draw is within expected limits.

Develop an algorithm to analyze the current data and detect any anomalies that may indicate energy theft. For example, if the current draw remains constant during non-peak hours or exceeds a certain threshold during peak hours, it may indicate unauthorized usage.

Integrate the system with other devices, such as a smart meter or a notification system, to take action if energy theft is detected. This could involve alerting the utility company or disconnecting the service to the premises.

It is worth noting that while the ACS712 current sensor can be a helpful component of a system for detecting and preventing energy theft, there needs to be a complete solution. Other components, such as smart meters, tamper-proof seals, and physical inspections, are also necessary to address the issue of energy theft effectively.

It connects the ACS712 current sensor with Arduino to detect and prevent energy theft. Follow these steps:

Connect the ACS712 sensor to the Arduino board as follows:

- Connect the VCC pin of the sensor to the 5V pin on the Arduino board.
- Connect the GND pin of the sensor to the GND pin on the Arduino board.
- Connect the sensor's OUT pin to analogue input pins on the Arduino board (for example, A0).

Write a program in the Arduino Integrated Development Environment (IDE) to read the analogue voltage output of the sensor using the analogRead() function.

Convert the analogue voltage readings to current values using the sensor's sensitivity factor, typically 185 mV/A for the ACS712-05A model.

Implement an algorithm to analyze the current data and detect anomalies indicating energy theft, such as constant current draw during non-peak hours or current draw exceeding a certain threshold during peak hours.

Integrate the system with other devices, such as a notification system or a relay, to take action if energy theft is detected.

## IV. Results

The system comprises an ATMega328 microprocessor, a 16x32 LED display, a battery-backed time and date sensor, and a power supply. The microcontroller controls the screen and constantly interacts with the date/time sensor. The battery backup keeps the system's time and date accurate in the case of a power interruption provided by the power source.

The code below provides an Arduino board's basic current sensing program using the ACS712-05A current sensor. The ACS712-05A is a hall effect current sensor, which can measure current in both directions.

This code will allow you to measure and monitor current in real-time for any device connected to the sensor. The primary applications of such a setup could be:

Real-Time Power Monitoring: The system can provide insights into the device's power consumption, which could be helpful in energy auditing or optimizing energy usage.

Safety: By keeping a record of how much electricity is being used, the system can spot problems like a short circuit, an overload, or a broken device.

Control Systems: In specific applications, this data could be used as feedback in control systems. For instance, current feedback can be used to control motor torque in a motor control system.

***Here is a code to get started:***

*CSharp*
*Copy code*

```
const int sensor in = A0; // Connect the ACS712 OUT pin to A0
const float sensitivity = 0.185; // Sensitivity factor for ACS712-05A model

void setup() {
  Serial.begin(9600); // Initialize serial communication for debugging
}

void loop() {
  int sensor value = analogRead(sensor in); // Read analog voltage output from sensor
  float current = (sensor value - 512) * (5.0 / 1023.0) / sensitivity; // Convert voltage to current value
  Serial.print("Current (A): ");
  Serial.println(current); // Print current value to serial monitor for debugging
  delay(1000); // Wait for 1 second before taking the next reading
}
```

This simple Arduino program reads the voltage output from the ACS712 current sensor and converts it into a current reading. This reading is then sent out to the Serial Monitor every second. Connecting the Arduino to a computer allows these current readings to be viewed in real time on the Arduino IDE's Serial Monitor.

Based on these estimates, a simple system consisting of an ACS712 sensor and an Arduino board would require a power

supply of 5V and consume around 1.5 mA (sensor) + 50 mA (Arduino) = 51.5 mA.

A power supply with a higher current rating than the estimated maximum current draw is recommended. For example, a 1A power supply would be sufficient for most small to medium-sized systems.

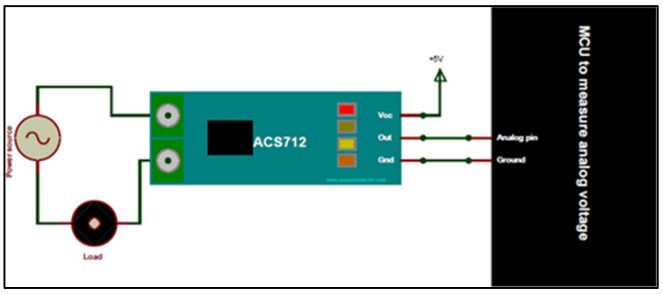


Fig. 4. Connecting the sensor to the Arduino

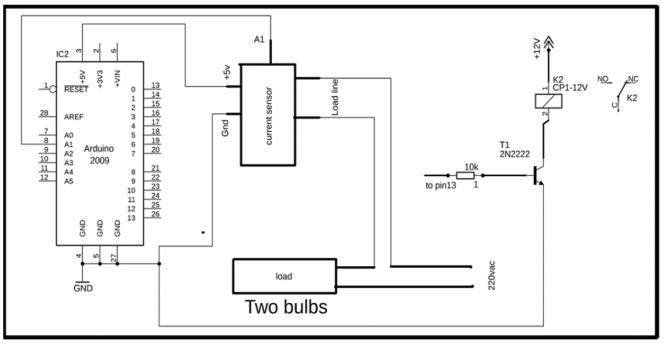


Fig. 5. Connect the circuit.

The pinout of a relay may vary depending on the specific model and manufacturer, but generally, a relay has the following pinout:

**Coil terminals:** The coil terminals connect the control signal that activates the relay. There are typically two coil terminals, one for positive voltage and one for negative or ground. When a voltage is applied to the coil, it generates a magnetic field that pulls the relay contacts.

**Common contact:** The common contact is the centre pin of the relay and is connected to one of the load terminals. When the relay is activated, the common contact switches from one load terminal to another, connecting or disconnecting the load.

**Normally open (NO) contact:** The normally open contact is connected to the standard contact when the relay is not activated. When the relay is activated, the normally open contact switches to the other load terminal, closing the circuit and connecting the load.

**Normally closed (NC) contact:** The normally closed contact is connected to the standard contact when the relay is not activated. When the relay is activated, the normally closed contact switches to an open circuit, disconnecting the load.

It is important to note that the pinout may vary between relays, and it is vital to refer to the datasheet or manual of the specific relay used to ensure proper connection. The following figure shows the relay module pinout.

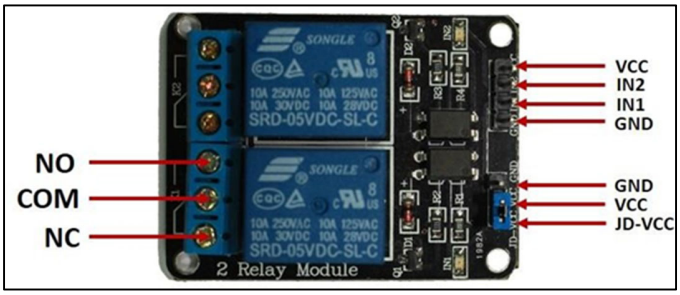


Fig. 7. Relay pin

Each of the two high-voltage connections has three available contacts: common (COM), usually closed (NC), and ordinarily open (NO).

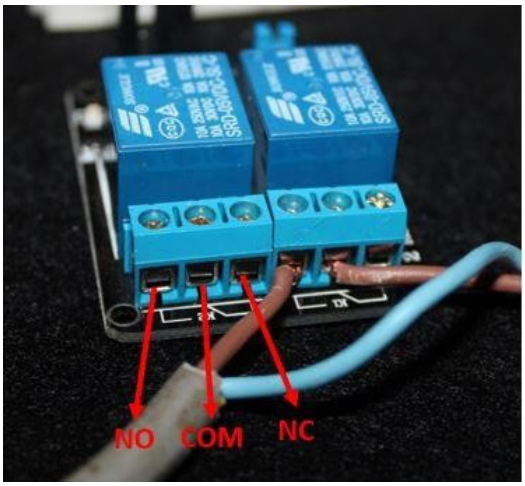


Fig. 8. Power connects

The experiment shows that it is possible to design and implement an efficient system for detecting and preventing energy theft in the power distribution network. This can help improve the quality of the power supplied to legal users, reduce the number of equipment failures, and prevent energy providers from suffering revenue losses. The result significantly affects decision-makers, energy providers, and the general public. This is because implementing the system can assist in resolving the problem of energy theft and ensure that everyone has access to high-quality, uninterrupted power.

With the help of an ATMega328 microcontroller, we can manipulate a 16x32 LED display and show animated messages, the time, and the date. The LED screen is a high-contrast, full-color matrix display. A battery-operated time and date sensor is included in the project so that information may be saved even if the electricity goes off.

Fig. 9. Project figure

The device also has a user interface where one may alter the date and time and design their visuals and messages to be shown on the LED screen.

This project shows how to use an ATMega328 microcontroller to manage and display animated messages, time, and date on a 16x32 LED display. A time and date sensor with a battery backup is included in the system to prevent the loss of time and date information during a power outage. Several uses may be found for this project, including public-area advertising, announcements, and time/date displays. The article's results are a great example of combining microcontrollers with LED displays to make exciting and educational displays.

## V. Discussion

The article thoroughly examines the significant problem of power theft and suggests a solution centred on smart meter technology to manage and deter such occurrences efficiently. The present study utilizes a wide range of academic literature. It employs advanced technology to tackle the urgent issues associated with energy theft, significantly contributing to the power distribution industry [37].

The study focuses on several complex obstacles related to energy theft, including technical and non-technical elements. A comprehensive analysis is conducted to assess the economic ramifications of this matter on the electricity grid and the broader Indian economy. Non-technical losses, specifically, have become a significant issue for power utilities, prompting the creation of effective detection methods to reduce financial losses and guarantee the reliability and longevity of the energy supply [38].

Authors in the area have presented numerous procedures and approaches to address the issue of energy theft, which are thoroughly examined in this article. One notable approach that has been considered is implementing a multi-sensor energy theft detection framework in advanced metering networks. This framework dramatically improves the precision and dependability of identifying energy theft cases using many sensors, offering valuable data for analysis and facilitating well-informed decision-making [6].

The study also emphasizes the significance of security and privacy considerations concerning the intelligent grid, particularly in preventing energy theft. The statement emphasizes the importance of installing strong security measures to protect sensitive information and deter unwanted access to the power system [10].

Moreover, the study emphasizes the importance of artificial intelligence (AI) and machine learning (ML) methodologies in identifying energy theft. Scholars have investigated using artificial intelligence (AI) models to detect non-technical losses, including support vector machines, random forests, and deep learning. The algorithms demonstrate remarkable precision in identifying atypical usage patterns, allowing utility companies to promptly address instances of energy theft [4].

The article also includes probabilistic approaches for estimating technical and non-technical losses in distribution systems. These technologies enable utility companies to comprehend possible losses comprehensively and formulate efficient ways to mitigate them [7].

The significance of using data-driven methodologies, such as GIS-based data-driven random forests and maximum entropy models, is emphasized. The use of data-driven models may be expanded to include the field of power theft detection. These models can spot abnormalities using consumption data patterns and trends [22].

Furthermore, the study combines several technologies, including computer vision and spatial and temporal deep learning, to detect non-technical power losses. The aforementioned cutting-edge technologies provide utilities with sophisticated functionalities, enabling them to evaluate extensive volumes of data and identify instances of energy theft with unmatched accuracy [26].

The article highlights the need for a comprehensive strategy for addressing energy theft. The statement underscores the importance of technical progress and the use of artificial intelligence (AI), machine learning (ML), and deep learning algorithms in the creation of intelligent systems that can effectively detect and mitigate instances of unlawful power usage [16].

The article provides insight into the significant problem of energy theft and its extensive ramifications for power providers and the broader economy. This study significantly contributes to energy theft detection and prevention by examining several approaches and modern technology, providing vital insights for creating efficient systems. Integrating innovative meter-based methodologies with artificial intelligence and machine learning methods can significantly augment the precision and effectiveness of energy theft identification. Consequently, this capability allows utilities to promptly implement measures, protect their financial assets and resources, and facilitate the transition towards a more stable and environmentally friendly energy landscape [35].

## VI. Conclusions

Creating and implementing a system capable of detecting and preventing energy theft in the power distribution network can be a game-changer in the ongoing battle against this recurrent issue in developing nations. The system, comprised of sensors, communications equipment, and software algorithms, can monitor energy consumption patterns, identify any

anomalies that may suggest theft, and send warnings to the appropriate authorities if there is a possibility of theft in the area.

This system has the potential to cut lost revenues for energy suppliers drastically, enhance the quality of electricity delivered to legitimate users, and minimize equipment failures due to overloading. All three of these benefits are possible because of the system's capabilities. Companies that depend on a consistent and dependable energy supply are less likely to suffer income losses, which is another benefit. The system may assist in guaranteeing everyone has accessibility to consistent electricity of high quality by locating instances of energy theft and taking measures to stop them.

The study emphasizes the possibility of this framework to make life better for all users while reducing the burden on the power distribution network. The study demonstrates that it is feasible to design and implement an effective system for detecting and preventing energy theft in the power distribution network. The findings of this research have significant repercussions for decision-makers, energy providers, and the general public. This is because implementing the system can assist in resolving the problem of energy theft and ensure that everyone has access to high-quality, uninterrupted power. In general, the development and implementation of this system have the potential to be a significant step toward the creation of an energy distribution network that is more sustainable and egalitarian.

An enormous and good influence has been made on the economy, the quality of life, and the environment as a result of the system that detects and prevents energy theft. Theft of energy is a criminal violation, and the damage it does to the economies of developing nations cannot be understated. The income losses that energy suppliers experience make it difficult for them to maintain and expand the power distribution network. This, in turn, results in poor power quality and availability for those who are legally allowed to use it.

The framework for identifying and avoiding energy robbery can help minimize lost revenues for power utilities, enhance the power delivered to regular users, and protect against equipment breakdown caused by overloading. These benefits come from the system's ability to detect and prevent energy theft. Businesses that rely on a steady and dependable power supply will be OK with the system since it can identify and prevent energy theft. It will assist in guaranteeing that these enterprises are not harmed. In addition, deploying the system may assist in lessening the load placed on the power distribution network, ultimately resulting in more renewable energy distribution networks.

In addition, the installation of the system has the potential to benefit the environment by lowering the need for extra power production to compensate for the energy lost due to theft. It is essential to use energy effectively in the battle against changing climate, and installing the system may assist in accomplishing this objective.

In conclusion, installing a system that can identify and prevent energy theft is essential in enhancing energy distribution networks in developing nations. Implementing the system may assist in cutting budget shortfalls for energy suppliers, enhance the quality of electricity delivered to legal users, and minimize equipment breakdowns caused by overloading. Also, it may result in energy distribution networks that are more environmentally friendly and have a constructive effect on the natural world. The system can guarantee that everyone has access to continuous electricity of high quality if energy theft is prevented. It would boost economic activity and development in these nations.

## REFERENCE


[1] T. Somuncu, and C. Hannum: ‘‘The Rebound Effect of Energy Efficiency Policy in the Presence of Energy Theft’’, *Energies*, 11, (12), 2018, pp. 3379

[2] O. Yakubu, N. Babu C, and O. Adjei: ‘‘Electricity theft: Analysis of the underlying contributory factors in Ghana’’, *Energy Policy*, 123, 2018, pp. 611-18

[3] R. Niu, J. Liu, X. Zhang, W. Guo, and B. Pan: ‘Research on Risk Analysis Technology of Electricity Stealing Behavior Characteristics in Smart Grid’, in Editor (Ed.)^(Eds.): ‘Book Research on Risk Analysis Technology of Electricity Stealing Behavior Characteristics in Smart Grid’ (2022, edn.), pp. 128-31

[4] A. Ullah, N. Javaid, M. Asif, M. U. Javed, and A. S. Yahaya: ‘‘AlexNet, AdaBoost and Artificial Bee Colony Based Hybrid Model for Electricity Theft Detection in Smart Grids’’, *IEEE Access*, 10, 2022, pp. 18681-94

[5] I. Rawtaer, R. Mahendran, E. H. Kua, H. P. Tan, H. X. Tan, T.-S. Lee, and T. P. Ng: ‘‘Early Detection of Mild Cognitive Impairment With In-Home Sensors to Monitor Behavior Patterns in Community-Dwelling Senior Citizens in Singapore: Cross-Sectional Feasibility Study’’, *J Med Internet Res*, 22, (5), 2020, pp. e16854

[6] S. K. Singh, R. Bose, and A. Joshi: ‘Energy theft detection in advanced metering infrastructure’, in Editor (Ed.)^(Eds.): ‘Book Energy theft detection in advanced metering infrastructure’ (2018, edn.), pp. 529-34

[7] R. Qi, J. Zheng, Z. Luo, and Q. Li: ‘‘A Novel Unsupervised Data-Driven Method for Electricity Theft Detection in AMI Using Observer Meters’’, *IEEE Transactions on Instrumentation and Measurement*, 71, 2022, pp. 1-10

[8] B. Atems, and C. Hotaling: ‘‘The effect of renewable and nonrenewable electricity generation on economic growth’’, *Energy Policy*, 112, 2018, pp. 111-18

[9] S. K. Singh, R. Bose, and A. Joshi: ‘‘Energy theft detection for AMI using principal component analysis based reconstructed data’’, *IET Cyber-Physical Systems: Theory & Applications*, 4, (2), 2019, pp. 179-85

[10] D. Yao, M. Wen, X. Liang, Z. Fu, K. Zhang, and B. Yang: ‘‘Energy Theft Detection With Energy Privacy Preservation in the Smart Grid’’, *IEEE Internet of Things Journal*, 6, (5), 2019, pp. 7659-69

[11] J. Pereira, and F. Saraiva: "Convolutional neural network applied to detect electricity theft: A comparative study on unbalanced data handling techniques," *International Journal of Electrical Power & Energy Systems*, 131, 2021, pp. 107085

[12] S. F. Hussain, H. Z. U. D. Babar, A. Khalil, R. M. Jillani, M. Hanif, and K. Khurshid: ‘‘A Fast Non-Redundant Feature Selection Technique for Text Data’’, *IEEE Access*, 8, 2020, pp. 181763-81

[13] A. Prakash, A. Shyam Joseph, R. Shanmugasundaram, and C. S. Ravichandran: ‘‘A machine learning approach-based power theft detection using GRF optimization’’, *Journal of Engineering, Design and Technology*, ahead-of-print, (ahead-of-print), 2021

[14] A. M. J. A.-A. Nameer Hashim Qasim, Haidar Mahmood Jawad, Yurii Khlaponin, Oleksandr Nikitchyn: ‘‘Devising a traffic control method for unmanned aerial vehicles with the use of GNB-IoT in 5G.’’, *Eastern-European Journal of Enterprise Technologies*, 117, (9), 2022, pp. 53-59

[15] Y. Gao, B. Foggo, and N. Yu: ‘‘A Physically Inspired Data-Driven Model for Electricity Theft Detection With Smart Meter Data’’, *IEEE Transactions on Industrial Informatics*, 15, (9), 2019, pp. 5076-88

[16] J. B. Leite, and J. R. S. Mantovani: ‘‘Detecting and Locating Non-Technical Losses in Modern Distribution Networks’’, *IEEE Transactions on Smart Grid*, 9, (2), 2018, pp. 1023-32

[17] Z. Zheng, Y. Yang, X. Niu, H. N. Dai, and Y. Zhou: ‘‘Wide and Deep Convolutional Neural Networks for Electricity-Theft Detection to Secure Smart Grids’’, *IEEE Transactions on Industrial Informatics*, 14, (4), 2018, pp. 1606-15

[18] P. O. Glauner, A. Boechat, L. Dolberg, J. A. Meira, R. State, F. Bettinger, Y. Rangoni, and D. Duarte: ‘‘The Challenge of Non-

Technical Loss Detection using Artificial Intelligence: A Survey'', *Int. J. Comput. Intell. Syst.*, 10, 2016, pp. 760-75
[19] R. Burgess, M. Greenstone, N. Ryan, and A. Sudarshan: ''The Consequences of Treating Electricity as a Right'', *Journal of Economic Perspectives*, 34, (1), 2020, pp. 145-69
[20] G. Micheli, E. Soda, M. T. Vespucci, M. Gobbi, and A. Bertani: "Big data analytics: an aid to the detection of non-technical losses in power utilities", *Computational Management Science*, 16, (1), 2019, pp. 329-43
[21] P. H. Li, C. H. Tsai, C. H. Chen, and P. C. Chen: 'High connectivity, low power, low cost advanced metering infrastructure', in Editor (Ed.)^(Eds.): 'Book High connectivity, low power, low cost advanced metering infrastructure' (2018, edn.), pp. 1-3
[22] S. C. Huang, Y. L. Lo, and C. N. Lu: ''Non-Technical Loss Detection Using State Estimation and Analysis of Variance'', *IEEE Transactions on Power Systems*, 28, (3), 2013, pp. 2959-66
[23] O. Rahmati, H. Pourghasemi, and A. Melesse: ''Application of GIS-based data driven random forest and maximum entropy models for groundwater potential mapping: A case study at Mehran Region, Iran'', *CATENA*, 137, 2015, pp. 360–72
[24] N. Qasim, Y. P. Shevchenko, and V. Pyliavskyi: "Analysis of methods to improve the energy efficiency of digital broadcasting", *Telecommunications and Radio Engineering*, 78, (16), 2019
[25] M. A. Shams, H. I. Anis, and M. El-Shahat: ''Denoising of Heavily Contaminated Partial Discharge Signals in High-Voltage Cables Using Maximal Overlap Discrete Wavelet Transform'', *Energies*, 14, (20), 2021, pp. 6540
[26] K. Costa, L. Pereira, R. Nakamura, P. R, J. Papa, and A. Falcão: ''A nature-inspired approach to speed up optimum-path forest clustering and its application to intrusion detection in computer networks'', *Information Sciences*, 294, 2015
[27] R. R. Bhat, R. D. Trevizan, R. Sengupta, X. Li, and A. Bretas: 'Identifying Non-technical Power Loss via Spatial and Temporal Deep Learning', in Editor (Ed.)^(Eds.): 'Book Identifying Non-technical Power Loss via Spatial and Temporal Deep Learning' (2016, edn.), pp. 272-79
[28] M. Geasa: "Development of an Arduino-based universal testing apparatus,", *Archives of Agriculture Sciences Journal*, 2022
[29] Y. K. Choi, J. H. Pak, K. Seo, S.-M. Jeong, T. Lim, and S. Ju: ''Realization of infrared display images using infrared laser projection method'', *Optics and Lasers in Engineering*, 145, 2021, pp. 106677
[30] M. H. Abd Wahab, N. Abdullah, A. Johari, and H. Abdul Kadir: ''GSM Based Electrical Control System for Smart Home Application'', *JCIT*, 5, 2010, pp. 33-39
[31] F. Kulor, D. E. Markus, M. W. Apprey, K. T. Agbevanu, and G. Gasper: ''Design and implementation of a microcontroller based printed circuit scrolling message notification board'', *IOP Conference Series: Materials Science and Engineering*, 1088, (1), 2021, pp. 012057
[32] M. Lv, G. Ou, and Z. Sun: ''Design and Realization of Test System for Digital Input and Output Module'', *Journal of Physics: Conference Series*, 2005, (1), 2021, pp. 012012
[33] D. V. Gadre, and S. Gupta: 'Analog to Digital Converter (ADC)', in Gadre, D.V., and Gupta, S. (Eds.): 'Getting Started with Tiva ARM Cortex M4
[34] Microcontrollers: A Lab Manual for Tiva LaunchPad Evaluation Kit' (Springer India, 2018), pp. 183-209
[35] A. D. Wickert, C. T. Sandell, B. Schulz, and G. H. C. Ng: ''Open-source Arduino-compatible data loggers designed for field research'', *Hydrol. Earth Syst. Sci.*, 23, (4), 2019, pp. 2065-76
[36] P. Ganguly, M. Nasipuri, and S. Dutta: ''A Novel Approach for Detecting and Mitigating the Energy Theft Issues in the Smart Metering Infrastructure'', *Technology and Economics of Smart Grids and Sustainable Energy*, 3, (1), 2018, pp. 13
[37] S. K. Gunturi, and D. Sarkar: "Ensemble machine learning models for the detection of energy theft,", *Electric Power Systems Research*, 192, 2021, pp. 106904
[38] D. Guarnizo-Peralta1: ''Disability rights in the Inter-American System of Human Rights'', *Netherlands Quarterly of Human Rights*, 36, 2018, pp. 43 - 63
[39] R. Baldwin, & di Mauro, B. W. (Eds.). (2020). . . . : ''Economics in the Time of COVID-19'', *American Journal of Industrial and Business Management*, 12, (7), 2022

```
const int currentPin = A1;  // current sensor connected with analog pin A1
const int relayPin = 13;    // relay connected to digital pin 13
const float loadThreshold = 2500.0;
const float calibrationFactor = 75.7576 / 1024.0;
const unsigned long sample time = 100000UL; // sample over 100ms, exact number of cycles for both 50Hz and 60Hz mains
const unsigned long numSamples = 250UL;    // divide sample time exactly, but low enough for the ADC to keep up
const unsigned long sampleInterval = sampleTime / numSamples; // the sampling interval
const int adcZero = 510; // relative digital zero of the arudino input from ACS712
bool isOverload = false;
void setup()
{
 Serial.begin(9600);
 pinMode(currentPin, INPUT);
 pinMode(relayPin, OUTPUT);
 digitalWrite(relayPin, LOW); // initial state
}
void loop()
{
 float current = getCurrent();
 Serial.print("Current: ");
 Serial.println(current);
 delay(1000);
 if (current >= loadThreshold && !isOverload)
 {
  isOverload = true;
  digitalWrite(relayPin, HIGH);
  Serial.println("Load exceeded! Power has been disconnected.");
 }
 if (current < loadThreshold && isOverload)
 {
  isOverload = false;
  digitalWrite(relayPin, LOW);
  Serial.println("Back to normal load. Power has been reconnected.");
 }
}
float getCurrent()
{
 unsigned long currentAcc = 0;
 unsigned int count = 0;
 unsigned long prevMicros = micros() - sampleInterval;
 while (count < numSamples)
 {
  if (micros() - prevMicros >= sampleInterval)
  {
   int adcRaw = analogRead(currentPin) - adcZero;
   currentAcc += (unsigned long)(adcRaw * adcRaw);
   ++count;
   prevMicros += sampleInterval;
  }
 }

 return sqrt((float)currentAcc / (float)numSamples) * calibrationFactor;
}
```