Design of an Automated Detection and Reporting System for Electricity Theft with Secure Recovery Mechanism

تصميم نظام آلي للكشف عن سرقة الكهرباء والإبلاغ عنها مع آلية إستعادة مؤمنه

Sideig Abdelrhman Ibrahim Dowi [1], Nahla Ibrahim Ali Taha [2]*, Mohamed Alnour Mustaffa[3]

[1]Dr, Nile Valley University – Sudan

[2*]Teaching Assistant, Shendi University – Sudan

[3]Dr, Nile Valley University – Sudan

*corresponding author: nahla13ibrahim@gmail.com

Abstract

Electricity theft is a major challenge for distribution companies, causing huge economic losses and instability in the electrical grid.

This research aims to design an automated system to ensure the immediate detection of electricity theft, automatic service disconnection, and safe remote reconnection.

The system was developed using an Arduino Uno microcontroller, where the system continuously monitors and compares the electrical power flowing in the company line and the user line.

Upon detecting a significant discrepancy, the system takes immediate action by automatically disconnecting the power supply via a relay and sending an alert notification via the GSM unit to the control center.

To address the issue of manually restoring service, the system offers an innovative solution it generates a random number of options and displays them on an LCD screen after receiving a payment confirmation signal from the control center.

The system was successfully simulated and tested using Proteus software, taking into account various scenarios: at different voltag levels (220,180,150,110) no load, normal load,theft. The results indicate that the proposed system is accurate and fast in detecting tampering and providing protection on distribution lines, offering a practical and effective solution to reduce electricity losses, enhance energy management efficiency, and decrease reliance on field human intervention.

Keywords: Global System for Mobile Communications(GSM), High Transmission Line(HTL), Liquid Crystal Display(LCD),Non-Technical Losses(NTL), Proteus, Simulation

المستخلص

تعد سرقة الطاقة الكهربائية تحديا كبيرا يواجه شركات التوزيع مما يتسبب في خسائر إقتصادية فادحة وعدم استقرار في الشبكة الكهربائية.

يهدف هذا البحث إلى تصميم نظام آلي لضمان الكشف الفوري عن سرقة الكهرباء، وفصل الخدمه تلقائيا، وإعادة التوصيل الآمن عن بعد.

تم تطوير النظام باستخدام متحكم دقيق اردوينو أونو، حيث يقوم النظام بمراقبة ومقارنه القدرة الكهربائية المتدفقه في خط الشركه وخط المستخدم بشكل مستمر.

عند اكتشاف فرق كبير يشير يتخذ النظام إجراء فورياً يتمثل في فصل التيار الكهربائي تلقائيا عن طريق مرحل ، وإرسال إشعار تنبيه عبر وحدة GSM إلى مركز التحكم .

لمعالجة مشكله إعادة الخدمة يدويا، يقدم النظام حلا مبتكرا يتمثل في توليد كلمه سر عشوائيا وعرضها على شاشة LCD بعد استلام إشارة تأكيد الدفع من مركز التحكم .

تمت محاكاة واختبار النظام بنجاح باستخدام برنامج بروتيوس مع الاخذ في الإعتبار سيناريوهات مختلفه عند مستويات جهد مختلفه(110،150،180،220) لايوجد حمل،الحمل طبيعي،سرقه. تشير النتائج أن النظام المقترح يتسم بالدقة والسرعة فى الكشف عن حالات التلاعب وتوفير الحمايه على خطوط التوزيع ، مما يوفر حلاًعمليًا وفعالا لتقليل الفاقد الكهربائي وتعزيز كفاءة إدارة الطاقة وتقليل الإعتماد على التدخل البشري الميداني.

Introduction

Electricity is the cornerstone of modern energy systems, powering vital sectors and services across all aspects of life. Delivering electricity efficiently to consumers requires an integrated infrastructure comprising generation plants, transmission and distribution networks, and metering systems. However, this infrastructure faces growing challenges-most notably electricity theft-which defined as the unauthorized use of electric power without proper payment.

There are various methods of electricity theft, Direct hooking from the mainline of a high transmission line is prevalent technique, accounting for 80% of worldwide electricity theft. In this method, consumers tap directly into the HTL without using the electricity meter panel.

Electricity theft detection is a critical issue due to its widespread prevalence and significant consequences. The impacts of electricity theft are substantial, including financial losses for utility companies, compromised service quality for legitimate consumers, reduced government revenue, system inefficiencies, and safety risks. Effectively addressing electricity theft requires advanced technologies, implementing robust detection systems and comprehensive strategies is crucial to protect revenue, ensure reliable service delivery, promote fairness, and maintain a sustainable energy distribution system.

The detection of electricity theft can be Traditional methods which are primarily from regular, and random, meter reader detection. Additionally, many utilities have anonymous reporting lines, and public informants are a reliable way to find thieves.

Traditional detection methods, such as manual inspections, are often inefficient, time-consuming, and prone to errors. Perpetrators employ sophisticated techniques to bypass detection, making it difficult to accurately identify instances of theft.

This research aims to address the existing gap by designing an automated system to ensure immediate and reliable detection of electricity theft. It provides an automated mechanism for remotely disconnecting and reconnecting service after verification of financial settlement, thus reducing reliance on field intervention by human operators.

System Design and Methodology

Block Diagram of the System

The system relies on two sensors, the first sensor is connected to the phase line coming from the electricity company, the second sensor is connected to the neutral line.
The Arduino Continuously compares the readings of both sensors, it sends a signal to the relay to disconnect the unauthorized load. Activates the buzzer to produce an audible alarm. Uses the GSM module to send an alert message. Displays the measured values directly on the LCD screen so the user can monitor consumption in real time. Employs a Push Button to enter numbers or commands instead of a traditional keypad. Figure 1 shows the block diagram of the system.

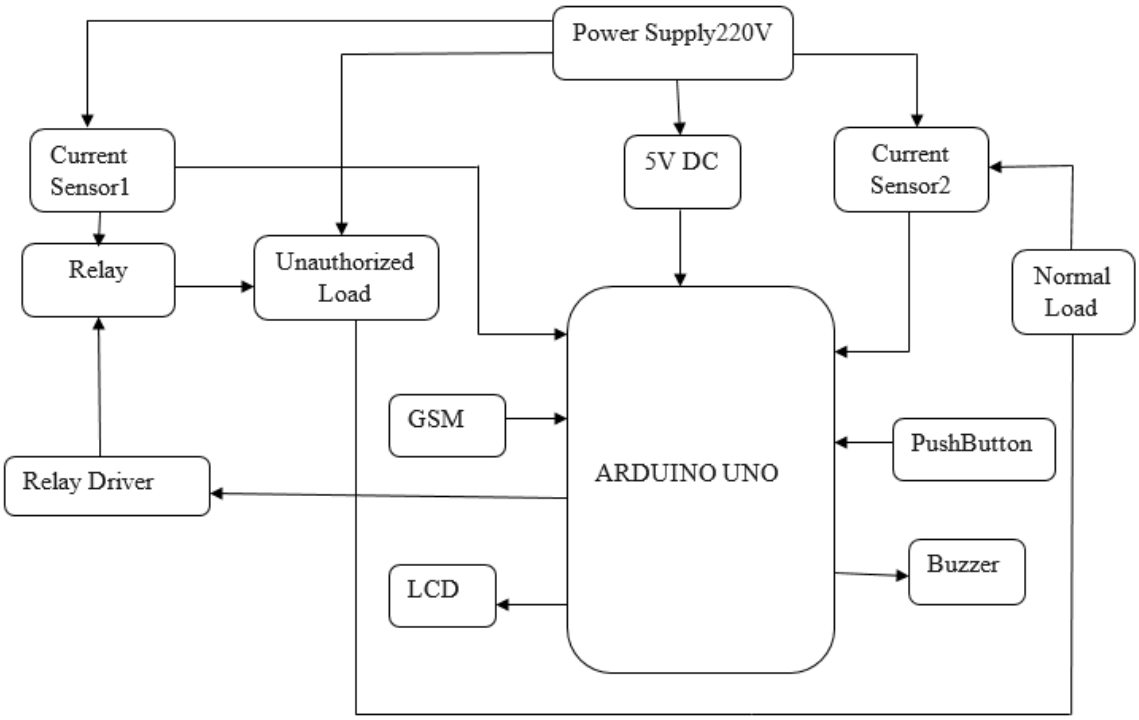


Figure 1**:** Block Diagram of the System.

Operation Mechanism and Algorithm

-The system begins with continuous monitoring by the Arduino using two precise current sensors.

-The Arduino reads the current values from these two sensors, and then calculates the electrical power on both sides every two seconds using the fundamental law of physics: Power = Voltage *Current*PF.

-When it detects that the user's consumption significantly exceeds the company's readings, it immediately cut off the electricity to the house via a relay.

-Meanwhile, an algorithm programmed within the Arduino calculates an immediate fine based on the amount of electricity stolen. Assumed as Fine = [(P-Company – P-User) / 220] × 100

-All these details are clearly displayed on an LCD screen connected to the Arduino.

-The system transmits detailed data about the theft including the value of the stolen current, power, and fine to the main control center via a GSM communication module.

-To restore service, the fine must first be paid through the designated channels. Upon receiving payment confirmation via the GSM module connected to the Arduino, the microcontroller generates a unique, randomly generated four-digit password. Figure 2 shows the Flowchart of the system.

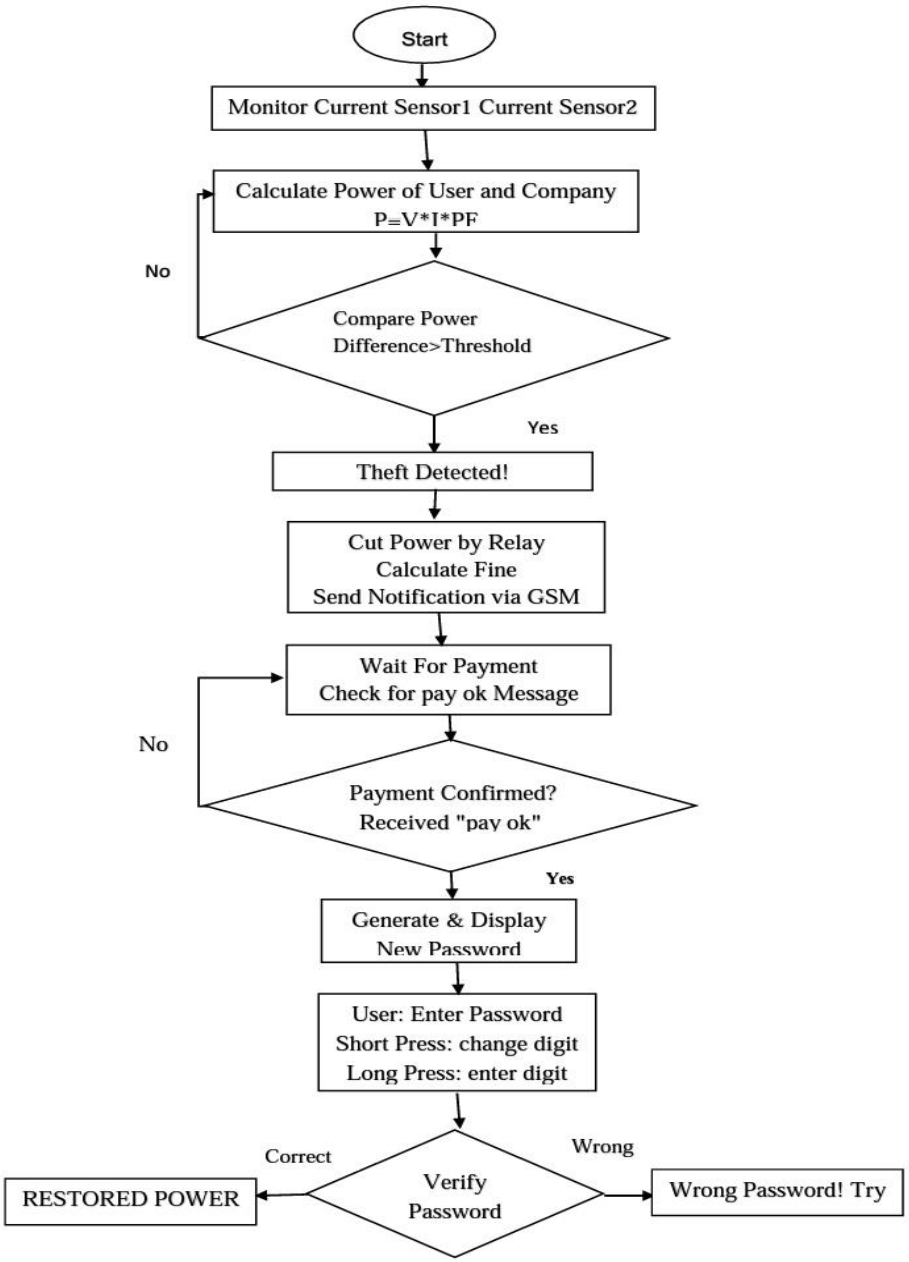


Figure 2: Flow Chart of the System.

Simulation Environment Results and Analysis

The electronic circuit was built using the Proteus simulation software, relying on an Arduino Uno microcontroller as the system's core. The main components were connected as follows:

The LCD screen was connected to the microcontroller's digital pins 12, 11, 5, 4, 3, and 2 to transmit data and display readings, the company's current sensor was connected to analog pin A2, and the user's current sensor to analog pin A0, a GSM module was installed via pins 6 and 7 for transmission and reception, with a physical control button connected to pin 9 for direct interaction, a relay was installed on pin 8 to control the electrical load, an alarm was connected to pin 10 to emit audible alerts.

Figure 3 shows the Simulation Environment.

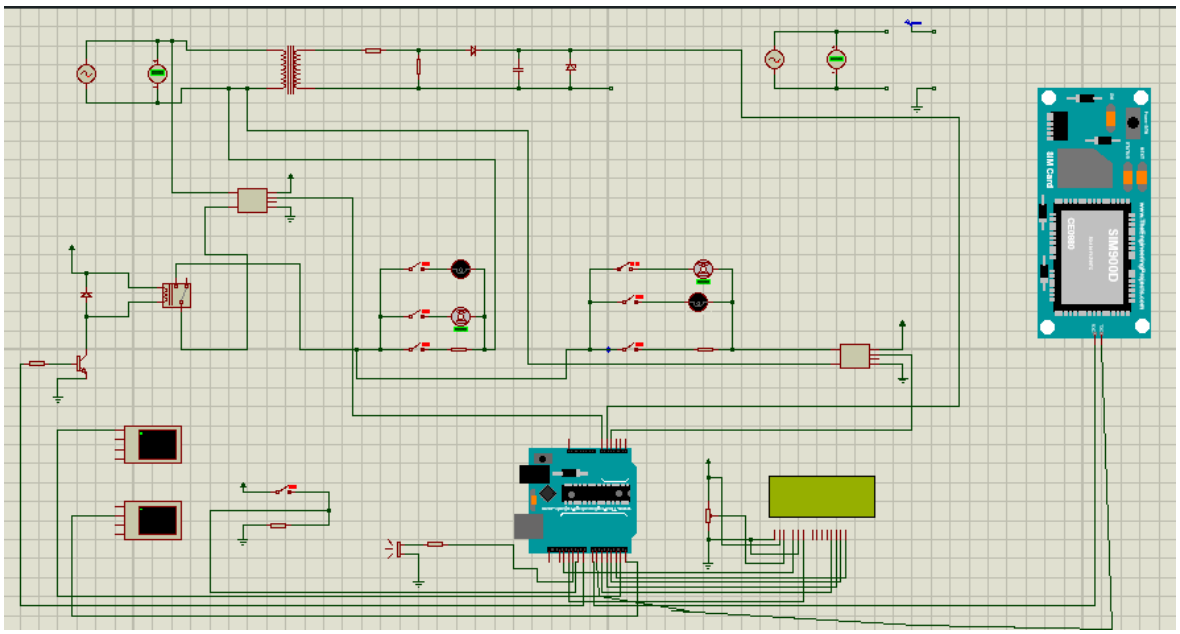


Figure 3:Simulation Environment.

When the circuit simulation is activated in the Proteus software and relay is on, then both the authorized and unauthorized loads will draw their own currents.

The system calculates energy consumption in kilowatts (kW) based on the current values detected by each current sensor (user and utility). Regarding the two system statuses:

i. Normal Status: The electrical load is properly connected downstream of the electricity meter and the user's current sensor, representing legitimate consumption (Authorized load).

ii. Theft Status: The load is directly connected to the 220V line upstream of the meter and sensors, representing electricity theft (Unauthorized load).

Simulation Results

the system was tested under four scenarios, from a no-load condition,

to a complex partial theft case, at different voltage levels(220,180,150,110).

Figure (4) 220 Volt- Four Scenarios(No load, Normal load, Theft load, Dual connection).

Figure (5) 180 Volt- Four Scenarios(No load, Normal load, Theft load, Dual connection).

Figure (6) 150 Volt- Four Scenarios(No load, Normal load, Theft load, Dual connection).

Figure (7) 110 Volt- Four Scenarios(No load, Normal load, Theft load, Dual connection).

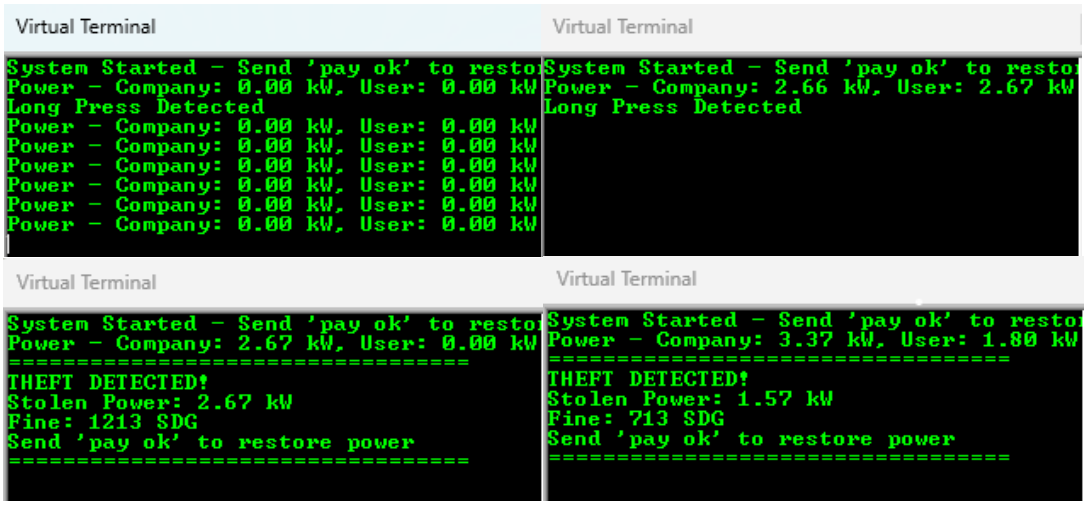


Figure 4: 220 Volt- Four Scenarios(No load, Normal load, Theft load,Dual connection).

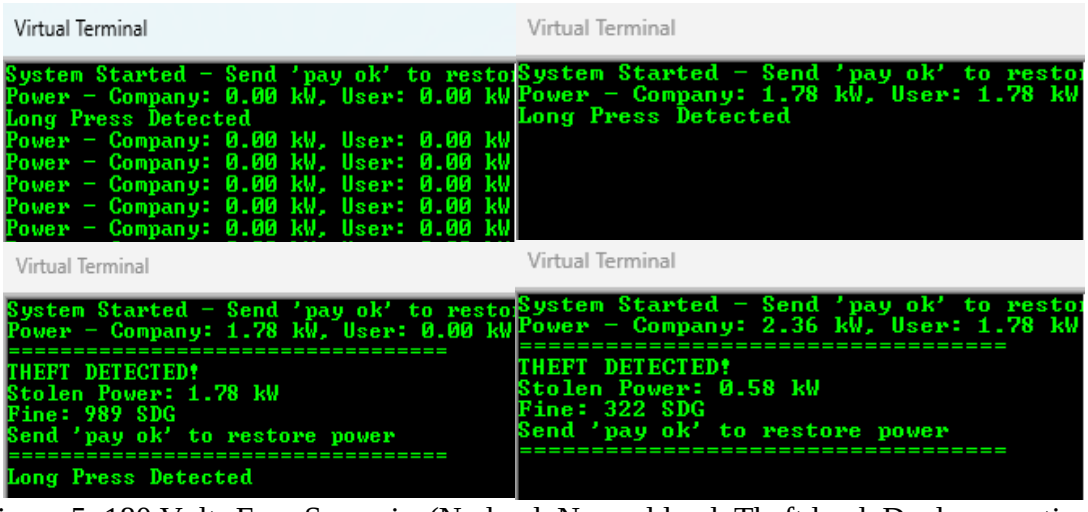


Figure 5: 180 Volt- Four Scenarios(No load, Normal load, Theft load, Dual connection).

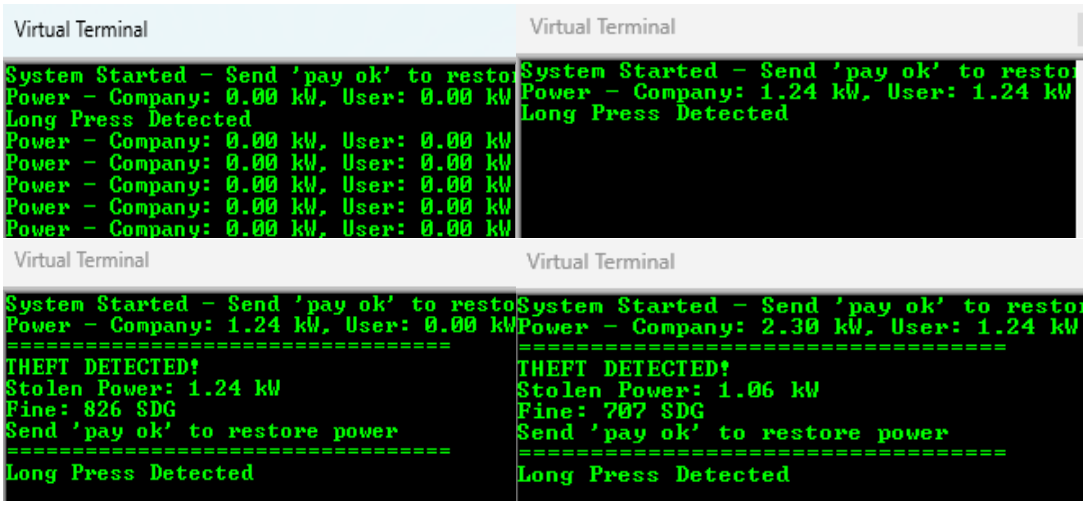


Figure 6: 150 Volt- Four Scenarios(No load, Normal load, Theft load, Dual connection).

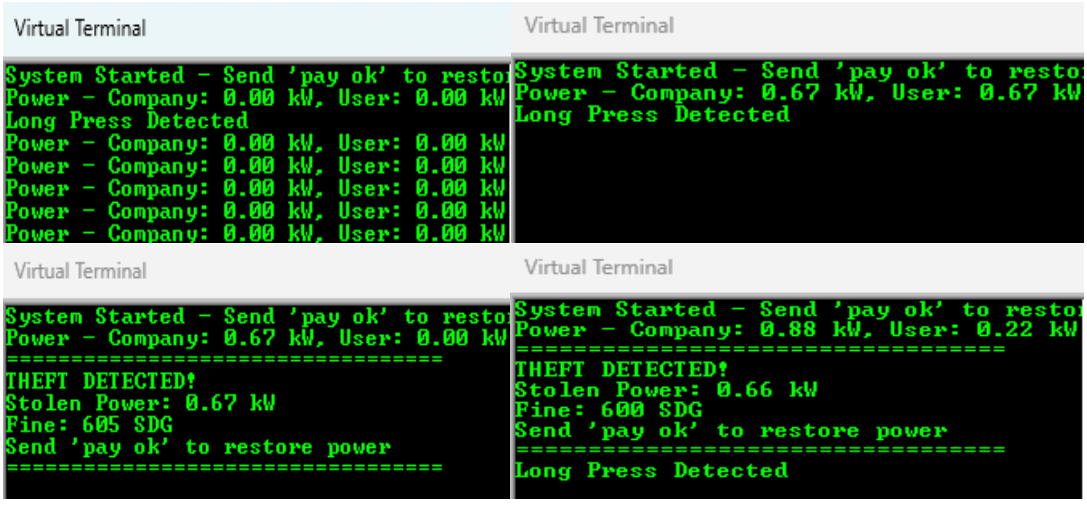


Figure 7: 110 Volt- Four Scenarios(No load, Normal load, Theft load, Dual connection).

Summary of Results

Table 1: Summary of the four core test scenarios at different voltage levels (220,180,150,110) designed to evaluate system performance under all realistic conditions.

Voltage	Scenarios	Company Power	User Power	Power Difference	Fine (SDG)
220V	Noload	0.00	0.00	0.0	0
	Normal load	2.66	2.67	0.01	0
	Theft load	2.67	0.00	2.67	1213
	Dual connect	3.37	1.80	1.57	713
180V	Noload	0.00	0.00	0.0	0
	Normal load	1.78	1.78	0.00	0
	Theft load	1.78	0.00	1.78	989
	Dual connect	2.36	1.78	0.58	322
150V	Noload	0.00	0.00	0.0	0
	Normal load	1.24	1.24	0.0	0
	Theft load	1.24	0.00	1.24	826
	Dual connect	2.30	1.24	1.06	707
110V	Noload	0.00	0.00	0.0	0
	Normal load	0.67	0.67	0.0	0
	Theft load	0.67	0.00	0.67	605
	Dual connect	0.88	0.22	0.66	600

Comparison of Power Difference with Voltage Drop Under Various Scenarios

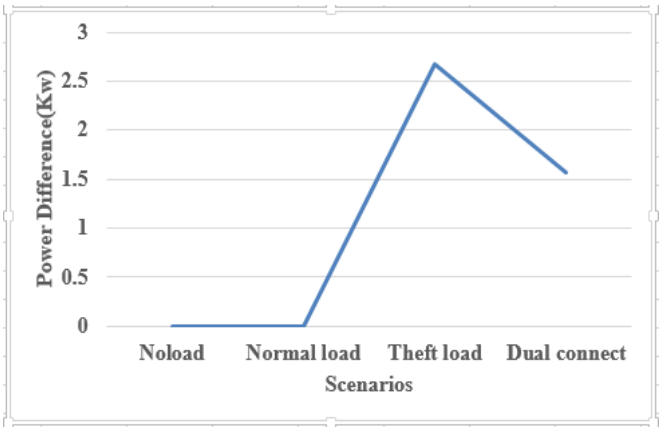


Figure8:Power Difference at 220Volt.

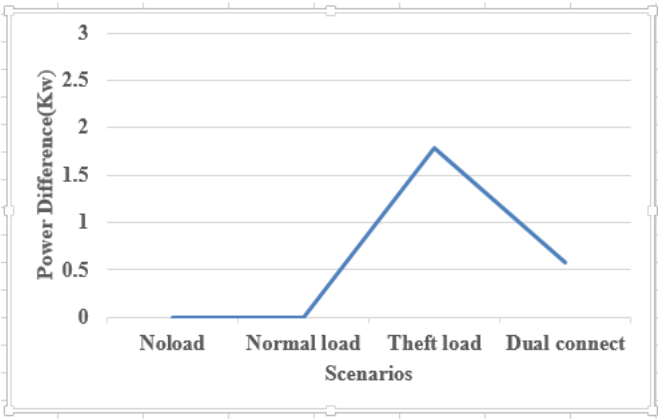


Figure9:Power Difference at 180Volt.

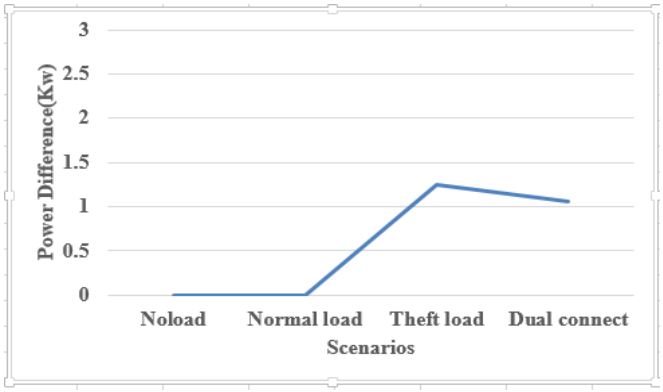


Figure10:Power Difference at 150Volt.

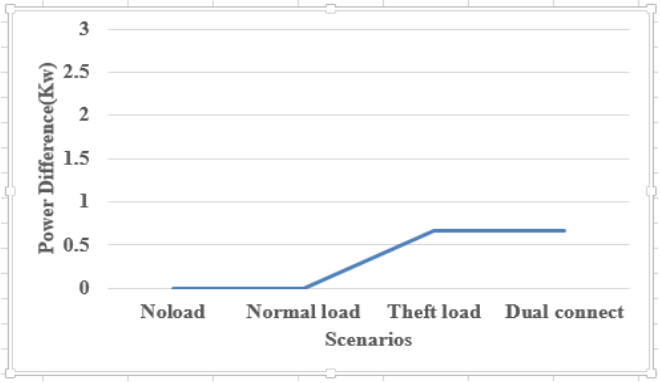


Figure11:Power Difference at 110Volt.

Analysis of Results

The results showed that the system achieved a detection accuracy of 100%, as it successfully detected all sixteen test cases at different voltage levels (220, 180, 150, and 110 V), with a constant response time of one second.

The results also showed that the difference between the measurements under normal operating conditions remained within the specified error margin (±1%), while this difference exceeded the error margin significantly in electricity theft cases. This enabled the system to distinguish between normal operating conditions and theft cases and make the detection decision correctly.Table2: Indicator of the system.

Performance Indicator	Result
Detection Accuracy	100%
Error Margin	±1%
Respons Time	1Second
Tested Voltage levels	220,180,150,110

Table3:Compare of Performance Indicators with previous studies on electricity theft detection.

Study	Components used	Scenarios	Accuracy	Time	Error Margin
Pallam et al.[1]	Dual energy meters (EM1,EM2) +Bluetooth+HC05 +GSMSIM800L+ Arduino Nano.	4scenarios (normal use,no use,full by pass,partial by pass)	95%	2-1 S	±5-8%
Oladele et al.[2]	3ACS712 current sensors+PIR tamper sensor +GSMSIM800L+ ESP32/Arduino Pro Mini+Android app	11theft scenarios+ normal senarios	98.7%	6-8S	±3.2% (thermal Drift ACS712)
Warade et al. [3]	3ACS712(30A) ZMPT101B voltage sensor+DS18B20 Temp sensor+ Arduion UNO+ ESP32Wi-Fi+Z-scoreML algorithm+MQTT+ Telegram	7 fault Categories+ direct and theft scenarios	95-97%	0.64-1.8 S	±2.1% (power) ±1.4% (voltage)

Payment Confirmation and Service Restoration Scenarios

After receiving payment confirmation from the control center via the GSM module, the scenarios on the user's screen are as follows: payment confirmation and password display as it shown in Figure 12; the user's failure to enter the password correctly, requiring a retry again and finally, the password being entered correctly, leading to the restoration of power to the user. Figures 13,14 show this scenarios.

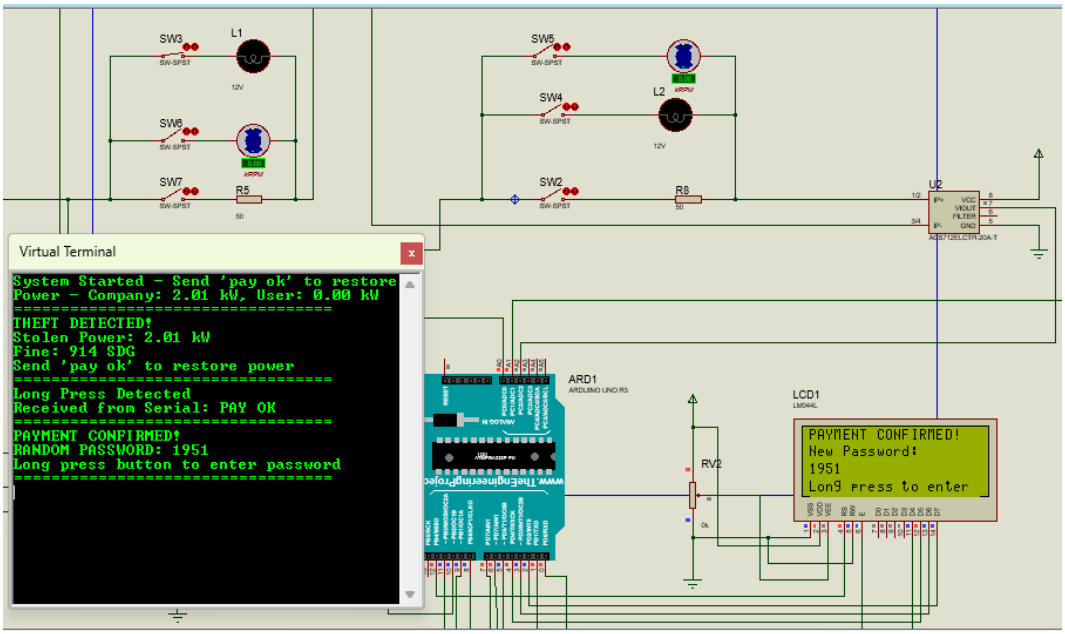


Figure 12: Payment Confirmation and Password Display Screen.

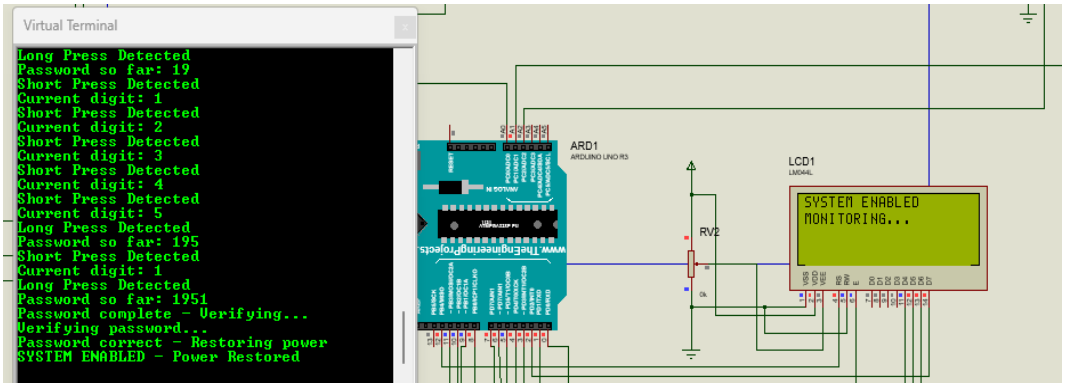


Figure 13: Successful Restoration Process Completion.

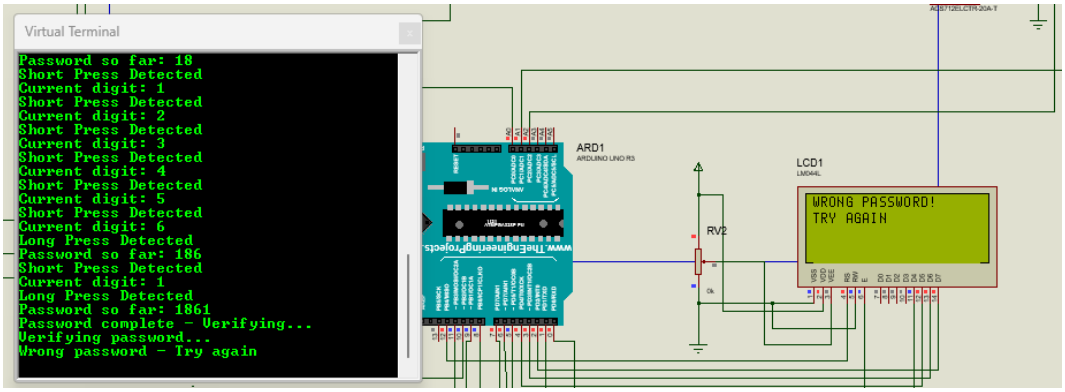


Figure 14: Verification Failure and Retry Again.

Conclusion

This paper developed an automated system for combating electricity theft, based on a microcontroller. The system aims to automatically monitor consumption, detect discrepancies between the company's and the user's current, and control the power supply accordingly. System simulations using Proteus software demonstrated high efficiency, accurately diagnosing various theft scenarios and immediately disconnecting the power supply. The system also features a proportional fine mechanism and a secure method for restoring service after payment.

It was also observed that the system maintained its stability, and the decrease in voltage did not cause any noticeable increase or decrease in system stability. Instead, it only resulted in a reduction in the measured power, proportional to the voltage decrease.

The paper offers a practical solution that contributes to reducing financial losses for distribution companies and provides a deterrent and fair mechanism for violators.

Among the most significant challenges encountered during implementation was the need to isolate the measurement circuits from electrical noise and ensure stable sensor readings.

References

[1] Charles Obasogie, Dr. Ibrahim M. Visa, Engr. Simon W. Pallam.(2023). “Automated Electricity Power Theft Identification and Reporting System”. International Journal of Science and Engineering Applications 12(05):2319-7560 . From: https://www.ijsea.com

[2] Oladele, Ojo Julius; Ariyo, Funso Kehinde; Ayanlade, Samson Oladayo; Adeagbo, Ayooluwa Peter; and Adeleke, Ismail Adeniyi. “ DEVELOPMENT OF AN IOT-BASED ENERGY THEFT DETECTION SYSTEM FOR A SINGLE-PHASE SMART METER”. Al-Bahir: Vol. 8: Iss. 1, Article 3. From: https://doi.org/10.55810/2313-0083.1120

[3] Om V. Warade, Trishul S. Sarode, Shruti R. Dikey, Tanuja N. Nemade, Prof. Nanda Y. Mhaisagar.(2026). “ IoT-Based Smart Energy Monitoring System with RealTime Theft Detection, ML Anomaly Analysis and Fault Protection”.IJIRT Volume 12 Issue 12 ISSN: 2349-6002.

Bibliography

[1] Md. Nazmul Hasan1,Rafia Nishat Toma1,Abdullah-AlNahid1 ,Jong-Myon Kim and M M Manjurul Islam. (2019). “Electricity theft detection in smart grid systems: A CNN-LSTM based approach”. Energies 12(17): 3310 . From: https://doi.org/10.3390/en12173310

[2] Zahoor Hussain, Shahzad Memon, Razahussain Shah, Zulfiqar Ali Bhutto, Mahmoud Aljawarneh. (2016). "Methods and techniques of electricity thieving in Pakistan". Journal of Power and Energy Engineering 4(9): 1-10. From: http://dx.doi.org/10.4236/jpee.2016.49001

[3] Bernat Coma-Puig , Josep Carmona, Ricard Gavald ,Santiago Alcoverro and Victor Martin. (2016). "Fraud detection in energy consumption: A supervised approach". In IEEE International Conference on Data Science and Advanced Analytics (DSAA); Canada pp 120-129. From: https://doi.org/10.1109/DSAA.2016.19

[4]YINING YANG,RUNAN SONG,YANG XUE,PENGHE ZHANG,YUEJIE XU, JINPING KANG (Member, IEEE),AND HAISEN ZHAO (Senior Member, IEEE). (2022). "A detection method for group fixed ratio electricity thieves based on correlation analysis of non-technical loss". IEEE Access 10: 5608-5619. From: https://doi.org/10.1109/ACCESS.2022.3141610

[5] Han, W., Xiao, Y.,. (2016). "Non-technical loss fraud in advanced metering infrastructure in smart grid". In International Conference on Cloud Computing and Security, pp. 163-172. From: https://doi.org/10.1007/978-3-319-48674-1_15

[6] Ibrahim Alotaibi,Mohammed A. Abido1, Muhammad Khalid and Andrey V. Savkin. (2020). "A comprehensive review of recent advances in smart grids: A sustainable future with renewable energy resources". Energies 13(23): 6269.

[7] Muhammad Salman Saeed, Mohd Wazir Mustafa,Nawaf N. Hamadneh, Nawa A. Alshammari ,Usman Ullah Sheikh,Touqeer Ahmed Jumani1,Saifulnizam Bin AbdKhalid and Ilyas Khan.(2020). "Detection of non-technical losses in power utilities-A comprehensive systematic review". Energies 13(18): 4727. From https://doi.org/10.3390/en13184727

[8] Fernando G.K. Guarda ,Bruno K. Hammerschmitt ,Marcelo B. Capeletti Laura L. C .dosSantos, Lucio R. Prade and Alzenira Abaide1 ,Nelson K. Neto .(2023). "Non-Hardware-BasedNon-Technical Losses Detection Methods: AReview". Energies,16, 2054. From: https:// doi.org/10.3390/en16042054

[9] Nizar Jabar Faqishafyee,Emad Hussen Sadiq, Harwan M.Tah.(2024). "Mitigating Non-Technical Losses and Electricity Theft Through Smart Meters: ACase Study of the Akre District Power Distribution Network".Journal of Intelligent Systems and Control pp 135-151. From: https://www.acadlore.com/journals/JISC

[10] B.V Surya Pavan , K. Kruthi Sai Amulya, J.Ramesh.(2019). " Detection of Power Theft using GSM" .Journal of Emerging Technologies and Innovative Research(JETIR) 6(5):2349-5162. From: https://www.jetir.org

[11] Charles Obasogie, Dr. Ibrahim M. Visa, Engr. Simon W. Pallam,(2023). "Automated Electricity Power Theft Identification and Reporting System". International Journal of Science and Engineering Applications 12(05):2319-7560. From: https://www.ijsea.com