IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A CLOUD BASED ENERGY AND FREQUENCY MONITORING SYSTEM USING IOT FOR THEFT DETECTION AND FORECASTING

Sathya Narayanan S, Raghul R, Suryaprakash S, Elango K

Department of Electrical and Electronics Engineering,
SRM Valliammai Engineering College, Kattankulathur, Chennai, India.

Abstract: The Internal and external power theft are detected the usage of the Prepaid Energy Meter with Theft Detection System. Internal power theft takes area after the power has reached the power meter, while outside power theft takes area earlier than the power has reached the power meter. The machine detects theft and additionally lets in customers to apply the pay as you go power meter feature. Users could be capable of pay earlier and utilize the suitable amount of power the usage of this feature The system begins with an IoT connection and configures the user's Internet settings first. When an external or internal theft occurs in the system, the system notifies the appropriate authority or user and updates the cloud. The system will also be Ables to save data when the prepaid balance is low or zero.

***Keywords* - ESP8266 Wi-Fi module, Energy Meter, IOT, Cloud server**

I. INTRODUCTION

For both power distribution companies and consumers, the Prepayment Energy's Meters is a valuable instrument for measuring electrical energy consumption. In addition, accelerated cognizance of the want for greater realistic electricity management, specifically withinside the location of electricity, necessitates an improve to this evaluation tool. Because the prepayment meter is an electronic device, it can keep track of events related to its activities in databases. Some of these records are only accessible through the keypad and the display on the screen in most classic prepayment meters. This is due to the facts that the meters were not designed to be wirelessly accessible and hence cannot be monitored remotely. Sending Shorts Messages Services (SMS) to the meters, for example, will not provide the unit balance or usage. Meters are also unable to record the last token recharging, the moment of a power outage, or restore on demand by SMS from mobile devices

The above-mentioned diagram depicts the paper's overall procedure. Things-on-the-internet Electricity billing system based on the Internet of Things. Electricity is purchased by the consumer based on his needs and credit. The hardware and software interfaces are connected to monitor the user's power usage, which will be tracked by IOT and delivered to the user who logs on to the webpage on the computer and the App on the mobile. The voltage, current, and power will be displayed on the smart meter's LCD display.

The SMS standard is supported by different communication networks, including the Global System for Mobile Communications (GSM), Code-Division Multiple Access (CDMA2000), and Digital Advanced Mobile Phone Service (DAMPS), according to research. They claimed in the publication that a wireless electricity theft detection systems based on Zigbee's technology is an efficient and less expensive approach to tamper with the wireless technique employed in this study. This wireless technology is used to prevent power theft by circumventing the energy meter, as well as to manage revenue losses and utility for the electricity authorized agency. Global energy challenges have been developing at an alarming rate in recent decades. As a result, a great deal of news technology has been introduced to meet user requests. In which the Energy Meter communicates the recorded power consumption reading via SMS services utilizing GSM technology. Power theft is on the rise as technology advances, which will have an impact on our country's economic stability.

A microcontroller is attached to an strength metering circuit, a GSM modem, and a contactor to makes or breaks energy strains in our system. MAX232 [4] is used to hyperlink the GSM modem to the microcontroller. If the stability is low or zero, it's miles utilized to ship a message to the stored tele cell smart phone number. We can use our cellular telephones to refill our strength meters, fending off overdue payments or pending payments.

For this study secondary data has been collected. From the website of KSE the monthly stock prices for the sample firms are obtained from Jan 2010 to Dec 2014. And from the website of SBP the data for the macroeconomic variables are collected for the period of five years. The time series monthly data is collected on stock prices for sample firms and relative macroeconomic variables for the period of 5 years. The data collection period is ranging from January 2010 to Dec 2014. Monthly prices of KSE -100 Index are taken from yahoo finance.

II. PROBLEM FORMULATION

This system has contributed a lot in giving awareness of electric consumption for users. Also, most systems have achieved in reducing the manpower involvement in the billing system since they are using GSM and web interfaces in notifying users their electricity consumption and bill. But still the current IoT based smart meters also have their own drawbacks.

- The above IoT smart meters are not stand alone they are generally interfaced on the traditional meters their power consumed isn’t always measured immediately which making the system less accurate.
- Most of the smart meter’s designs with inside the above report awareness on showing the quantity of strength fed on and calculating the invoice they don’t perform strength performance works.
- Most smart meters aren't operating on strength financial savings or growing strength performance best provide consciousness of the electricity consumed
- On most designs do not allow Users to control their load requirements
- Much needed to be done to secure energy data management issues
- Fault detection and theft detection methods are not accurate.

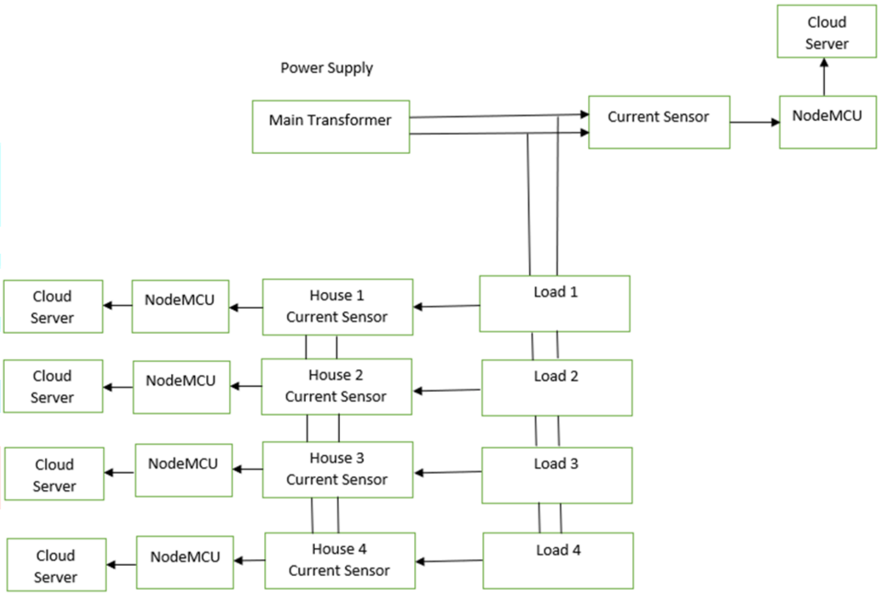


Fig. 1 Block diagram

Table. 1 Energy Reading for 2019

No. of Houses	Jan-Feb	March-April	May-June	July-Aug	Sep-Oct	Nov-Dec
House 1	80	95	100	90	110	120
House 2	180	170	165	190	200	230
House 3	800	730	700	790	850	900
House 4	300	400	200	180	290	350
House 5	120	150	280	**3850**	250	190
House 6	380	480	510	490	600	700
House 7	800	850	690	780	700	750
House 8	1100	1400	1700	2000	2100	1500
House 9	500	590	500	580	650	750
House 10	400	600	500	700	350	520

Table. 2 Energy Reading for 2020

No. of Houses	Jan-Feb	March-April	May-June	July-Aug	Sep-Oct	Nov-Dec
House 1	70	120	150	100	90	110
House 2	150	120	110	150	190	220
House 3	820	790	780	700	890	950
House 4	400	500	410	290	350	390
House 5	190	120	280	350	**3950**	150
House 6	390	450	550	480	650	750
House 7	850	820	750	710	720	740
House 8	1200	1500	1800	1320	2000	1755
House 9	600	450	480	380	520	710
House 10	550	650	450	660	550	450

Table. 3 Energy Reading for 2021

No. of Houses	Jan-Feb	March-April	May-June	July-Aug	Sep-Oct	Nov-Dec
House 1	50	70	40	65	90	85
House 2	150	180	210	230	170	240
House 3	750	690	680	780	800	820
House 4	250	350	180	150	280	310
House 5	100	120	**3150**	150	210	220
House 6	350	450	490	550	650	720
House 7	850	820	780	790	650	840
House 8	1200	1500	1600	1700	1900	2200
House 9	2200	2050	2350	2200	2150	2250
House 10	470	580	475	495	535	550

A Smarts Prepaids energy Metering Systems was created, installed, and tested in this article to identify energy theft through energy meter by-passing or tampering. If energy was stolen, the load's power supply would be turned off automatically. The advent of smart meters with expanded capabilities and functions represents a quantum's leaps forwards in the development of energy metering systems. It also includes the ability to measure current and voltage valued utilizing a data base for each load. Theft of energy makes up a significant portion of non-technical losses in power transmission and distribution.

- Users will be able to pay in advance and consume only the quantity of energy they require.
- To pinpoint the right location of energy theft in the area.
- These techniques cans be used to spot anomalous energy usage
- The system begins with an IoT Connection and configures the authority and user first

The energy theft can be identified by the comparing past 2-year energy consumption reading which is stored in the cloud. By comparing the usage of energy consumption in that who consume the energy, varies drastically high by the past 2 year. By analysis the data that energy consumer assumes to be theft. Theft can be found out by, if user consume energy more than maximum load of a transformer load supply which is more the given load supply to a particular house. A 25KVA transformer the power supply is distributed to 30 houses; each house maximum load current is 2KVA for single phase line. If there is three phase line maximum load is 4KVA- 5KVA. If user consumer more than the maximum load power supply, the theft can be identified by analyzing the past 2 year- 3-year energy consumption reading. Who energy consumption reading is the increase drastically for a particular time, it assumes to be energy theft. After identifying the theft, the user is given the penalty for illegal consumption of energy.

III. Implementation of Frequency MONITORING USING IoT

The standard IoT architecture the energy and frequency metering system were designed to show the communication between the utility and the residence through cloud. The system will have 3 basic parts the energy meter, communication unit and data storage and visualization unit.in this part the design of energy meter integrated with Wi-Fi module. The microcontroller detected how a good deal device the consumer have bought and the relay turned into switched accordingly. When the devices bought have become identical to the devices consumed, the relay completed its characteristic via way of means of switching off the strength system. The caution turned into dispatched to authority or consumer cell thru IOT generation earlier than the disconnection of strength. Hardware version is likewise designed the usage of IoT. Detection of electricity theft was also made possible by using this system, through which the server received the message when users passed the meter. In each house the energy meter is fixed with an additional Node MCU that helps to connect the cloud. The status of the energy meter is accessed. from the cloud to the microcontroller.

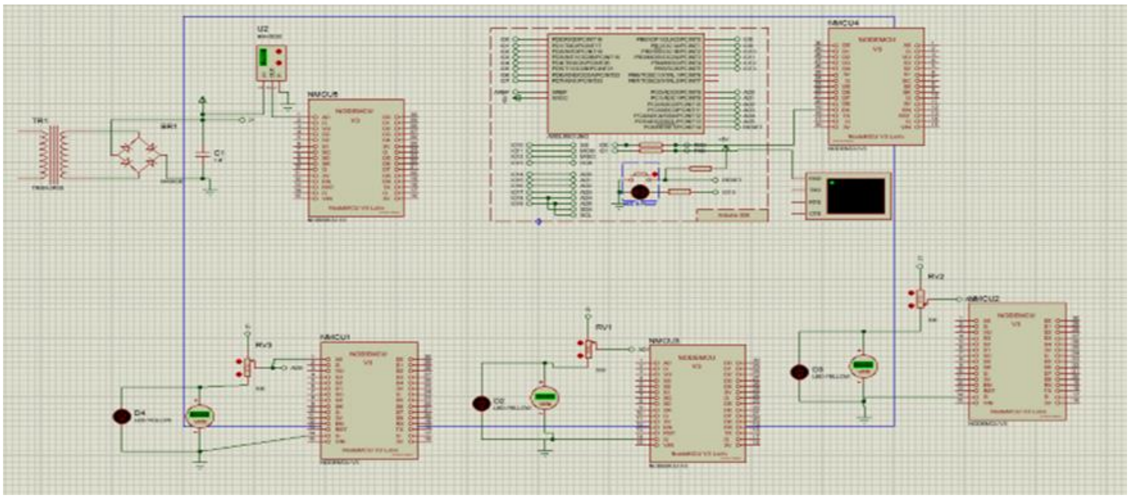
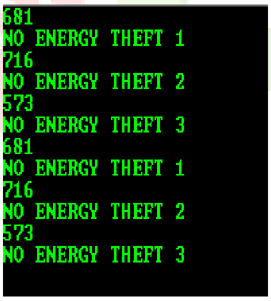


Fig.2. Simulation Diagram

The customers Realtime electricity intake facts wishes to be saved on cloud server in order that the consumer can without problems get admission to the intake and Tarif facts from everywhere plus the intake records may be beneficial for in addition evaluation purpose. Here we've used an open supply IoT platform referred to as ThingSpeak. That lets accumulate and keep sensor facts withinside the cloud and expand applications. ThingSpeak is an API and open-supply Internet of Things software to retrieve and keep facts from matters the use of the HTTP protocol via the network. The quantity of electricity intake facts saved withinside the cloud server, can used for detecting the robbery arise withinside the specific location. Each consumer house the energy and frequency meter are limked to cloud through node mcu, then it will be accessed to microcontroller through the internet. In Proteus software program simulation circuit is made. Mainly, the circuit may be divided into halves.

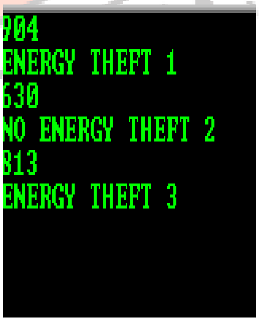
IV. RESULTS AND DISCUSSION

Using the cloud server, the energy consumption reading are access anywhere form the world. The energy consumption history is useful for analysis purpose to compare the data for past 2 year energy reading.Using this the theft may be pointed out. The alert machine for energy intake is hired to alert the client approximately variety of devices fed on daily. Fig. three constitute while no power robbery occurs, the person purchaser the energy wisely. Fig. 4 shows when energy theft is occurred, these can be find out when user consume more than the maximum load of energy, which is drastically increases for particular over of time. By using this method, the theft can be reduced.



```
681
NO ENERGY THEFT 1
716
NO ENERGY THEFT 2
573
NO ENERGY THEFT 3
681
NO ENERGY THEFT 1
716
NO ENERGY THEFT 2
573
NO ENERGY THEFT 3
```

Fig. 3 When No Energy Theft Occur



```
904
ENERGY THEFT 1
630
NO ENERGY THEFT 2
813
ENERGY THEFT 3
```

Fig. 4 When Energy Theft Occur

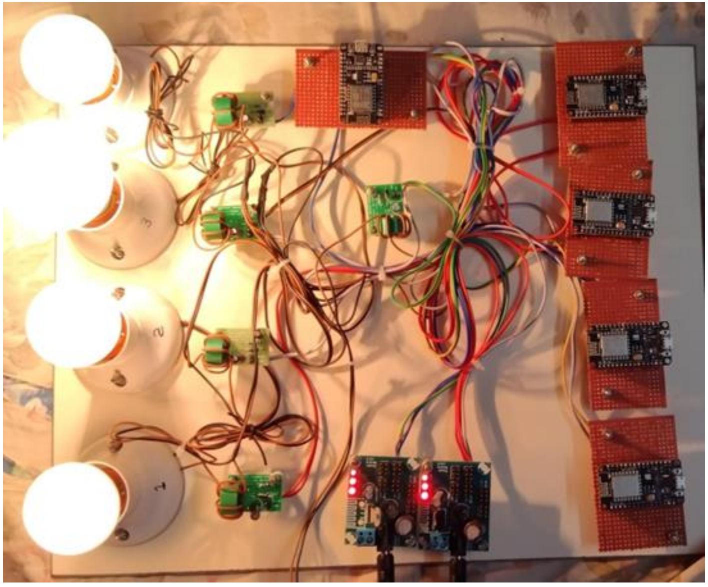
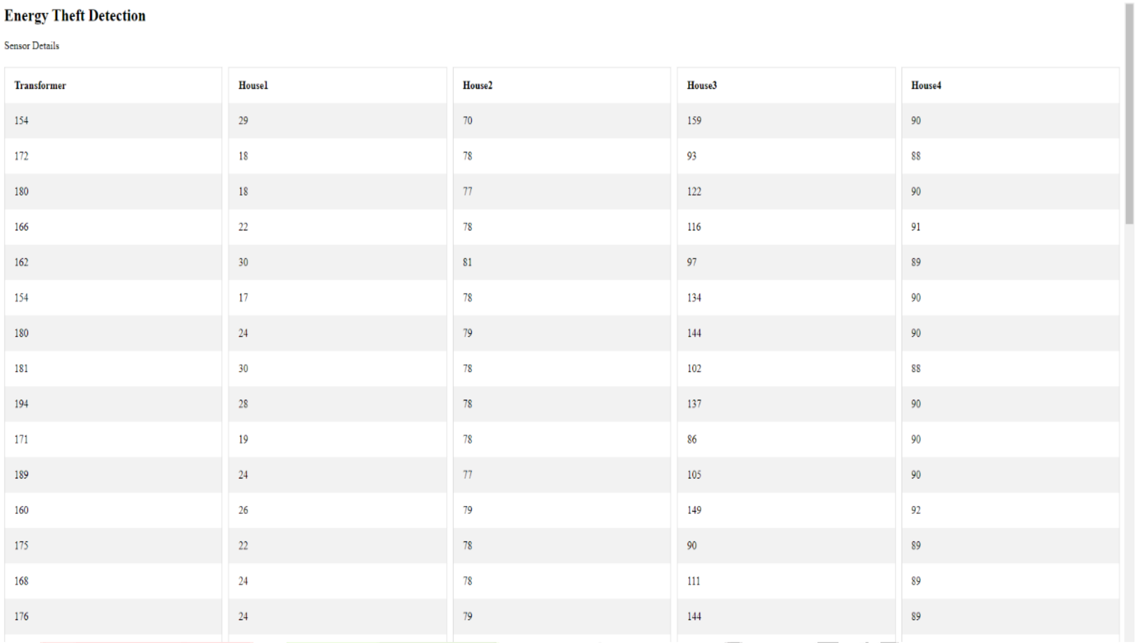


Fig.5. Hardware setup

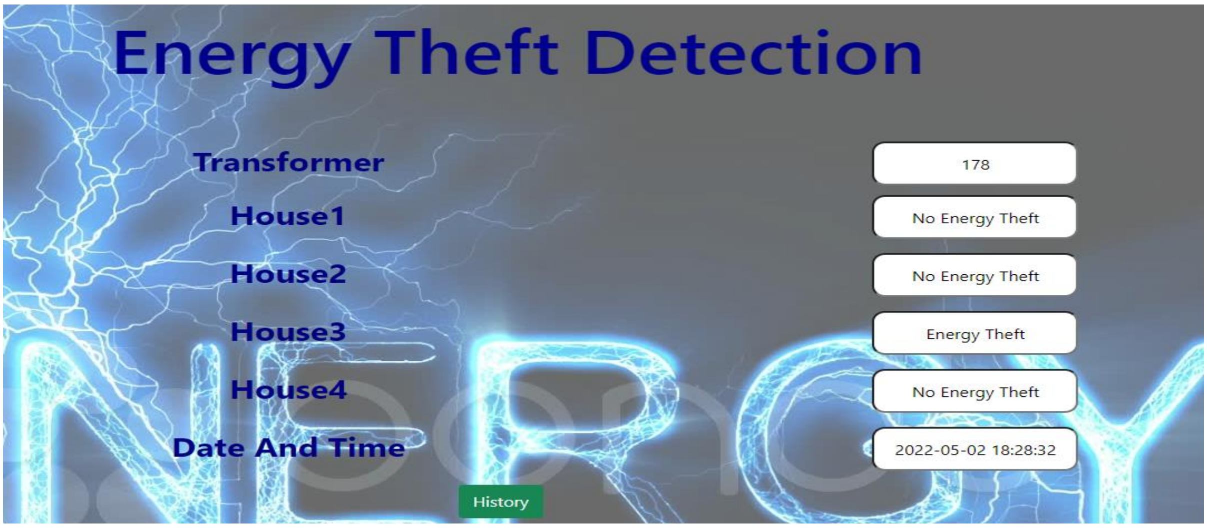


Energy Theft Detection

Sensor Details

Transformer	House1	House2	House3	House4
154	29	70	159	90
172	18	78	93	88
180	18	77	122	90
166	22	78	116	91
162	30	81	97	89
154	17	78	134	90
180	24	79	144	90
181	30	78	102	88
194	28	78	137	90
171	19	78	86	90
189	24	77	105	90
160	26	79	149	92
175	22	78	90	89
168	24	78	111	89
176	24	79	144	89

Fig.6. Data Stored In Cloud



Energy Theft Detection

Transformer: 178

House1: No Energy Theft

House2: No Energy Theft

House3: Energy Theft

House4: No Energy Theft

Date And Time: 2022-05-02 18:28:32

Fig.7. Webpage Result

REFERENCES

[1] D. Yao, M. Wen, X. Liang, Z. Fu, K. Zhang and B. Yang, “Energy Theft Detection With Energy Privacy Preservation in the Smart Grid”, IEEEInternet of Things Journal, Vol. 6, No. 5, pp. 7659-7669, Oct. 2019, DOI:10.1109/JIOT.2019.2903312.

[2] G. A. Raiker, Subba Reddy B, Umanand Loganathan, Shubham Agrawal, Anchal S Thaku, Ashwin K. John P. Barton, Murray Thomson, “EnergyDisaggregation Using Energy Demand Model and IoT-Based Control”, IEEE Transactions on Industry Applications, Vol. 57, No.2, pp. 1746-1754,March-April 2021, DOI:10.1109/TIA.2020.3047016.

[3] G. Giaconi, D. Gündüz and H. V. Poor, “Smart Meter Privacy With Renewable Energy and an Energy Storage Device”, IEEE Transactions onInformation Forensics and Security, Vol. 13, No. 1, pp. 129-142, Jan. 2018, DOI:10.1109/TIFS.2017.2744601

[4] H. Cai, B. Xu, L. Jianag and A. V. Vasilakos, “IoT-Based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges”, IEEEInternet of Things Journal, Vol. 4, No. 1, pp. 75-87, Feb. 2017, DOI:10.1109/JIOT.2016.2619369.

[5] H. Miao, G. Chen, Z. Zhao and F. Zhang, “Evolutionary Aggregation Approach for Multihop Energy Metering in Smart Grid for Residential EnergyManagement”, IEEE Transactions on Industrial Informatics, Vol. 17, No. 2, pp. 1058-1068, Feb. 2021, DOI:10.1109/TII.2020.3007318.

[6] L. De Oro Arenas, G. de Azevedo e Melo and C. A. Canesin, “A Methodology for Power Quantities Calculation Applied to an FPGA-Based SmartEnergy Meter”, IEEE Transactions on Instrumentation and Measurement, Vol. 70, pp. 1-11, 2021, No. 9000711, DOI:10.1109/TIM.2020.3034978.

[7] M. B. Gough, S. F. Santos, T. AlSkaif, M. S. Javadi, R. Castro and J. P. S. Catalão, “Preserving Privacy of Smart Meter Data in a Smart Grid Environment”, IEEE Transactions on Industrial Informatics, Vol. 18, No.1, pp. 707-718, Jan. 2022, DOI:10.1109/TII.2021.3074915.

[8] M. D. Wagy, J. C. Bongard, J. P. Bagrow and P. D. H. Hines, “Crowdsourcing Predictors of Residential Electric Energy Usage”, IEEE SystemsJournal, Vol. 12, No. 4, pp. 3151-3160, Dec. 2018, DOI:10.1109/JSYST.2017.2778144.

[9] M. Simonov, G. Chicco and G. Zanetto, “Event-Driven Energy Metering: Principles and Applications”, IEEE Transactions on Industry Applications,Vol. 53, No. 4, pp. 3217-3227, July-Aug. 2017, DOI:10.1109/TIA.2017.2679680.

[10] M. I. Ibrahem, M. Nabil, M. M. Fouda, M. M. E. A. Mahmoud, W. Alasmary and F. Alsolami, “Efficient Privacy-Preserving Electricity TheftDetection With Dynamic Billing and Load Monitoring for AMI Networks”, IEEE Internet of Things Journal, Vol. 8, No. 2, pp. 1243-1258,Jan.2021, DOI:10.1109/JIOT.2020.3026692.

[11] Marco Pau, Edoardo Patti, Luca Barbierato, Abouzar Estebsari, Enrico Pons, Ferdinanda Ponci, and Antonello Monti, “Design and Accuracy Analysisof Multilevel State Estimation Based on Smart Metering Infrastructure”, IEEE Transactions on Instrumentation and Measurement, Vol.68, No. 11, pp. 4300-4312, Nov. 2019, DOI:10.1109/TIM.2018.2890399.

[12] M. M. Albu, M. Sănduleac and C. Stănescu, “Syncretic Use of Smart Meters for Power Quality Monitoring in Emerging Networks”, IEEETransactions on Smart Grid, Vol. 8, No. 1, pp. 485-492, Jan. 2017, DOI:10.1109/TSG.2016.2598547.

[13] N. Duan, C. Huang, C. -C. Sun and L. Min, “Smart Meters Enabling Voltage Monitoring and Control: The Last-Mile Voltage Stability Issue”, IEEETransactions on Industrial Informatics, Vol. 18, No. 1, pp. 677-687, Jan. 2022, DOI:10.1109/TII.2021.3062628.

[14] P. Kumar, A. Gurtov, M. Sain, A. Martin and P. H. Ha, “Lightweight Authentication and Key Agreement for Smart Metering in Smart EnergyNetworks”, IEEE Transactions on Smart Grid, Vol. 10, No. 4, pp. 4349-4359, July 2019, DOI:10.1109/TSG.2018.2857558.

[15] Q. Yang and H. Wang, “Privacy-Preserving Transactive Energy Management for IoT-Aided Smart Homes via Blockchain”, IEEE Internet of ThingsJournal, Vol.8, No. 14, pp. 11463-11475, July 2021, DOI:10.1109/JIOT.2021.3051323.

[16] R. J. Tom, S. Sankaranarayanan and J. J. P. C. Rodrigues, “Smart Energy Management and Demand Reduction by Consumers and Utilities in an IoTFog-Based Power Distribution System”, IEEE Internet of Things Journal, Vol. 6, No. 5, pp. 7386-7394, Oct. 2019, DOI:10.1109/JIOT.2019.2894326.

[17] R. Morello, C. De Capua, G. Fulco and S. C. Mukhopadhyay, “A Smart Power Meter to Monitor Energy Flow in Smart Grids: The Role of Advanced Sensing and IoT in the Electric Grid of the Future”, IEEE Sensors Journal, Vol. 17, No. 23, pp. 7828-7837, 1 Dec.1, 2017, DOI:10.1109/JSEN.2017.2760014.

[18] S. Chakraborty and S. Das, “Application of Smart Meters in High Impedance Fault Detection on Distribution Systems”, IEEE Transactions on SmartGrid, Vol.10, No. 3, pp. 3465-3473, May 2019, DOI:10.1109/TSG.2018.2828414.

[19] V. C. Cunha, W. Freitas, F. C. L. Trindade and S. Santoso, “Automated Determination of Topology and Line Parameters in Low Voltage Systems Using Smart Meters Measurements”, IEEE Transactions on Smart Grid, Vol. 11, No. 6, pp. 5028-5038, Nov. 2020, DOI:10.1109/TSG.2020.3004096.

[20] Victor Andres Ayma Quirita, Gilson Alexandre Ostwald Pedro da Costa, Patrick Nigri Happ, Raul Queiroz Feitosa, Rodrigo da Silva Ferreira, Dario Augusto Borges Oliveira, and Antonio Plaza, “A New Cloud Computing Architecture for the Classification of Remote Sensing Data”, IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, Vol. 10, No. 2, pp. 409-416, Feb. 2017, DOI:10.1109/JSTARS.2016.2603120.

[21] V. B. Krishna, C. A. Gunter and W. H. Sanders, “Evaluating Detectors on Optimal Attack Vectors That Enable Electricity Theft and DER Fraud”, IEEEJournal of Selected Topics in Signal Processing, Vol. 12, No. 4, pp. 790-805, Aug. 2018, DOI:10.1109/JSTSP.2018.2833749.

[22] W. Li, T. Logenthiran, V. Phan and W. L. Woo, “A Novel Smart Energy Theft System (SETS) for IoT-Based Smart Home”, IEEE Internet of ThingsJournal, Vol. 6, No. 3, pp. 5531-5539, June 2019, DOI:10.1109/JIOT.2019.2903281.

[23] Y. You, Z. Li and T. J. Oechtering, “Energy Management Strategy for Smart Meter Privacy and Cost Saving”, IEEE Transactions on InformationForensics and Security, Vol. 16, pp. 1522-1537, 2021, DOI:10.1109/TIFS.2020.3036247.

[24] Yongdong Wu, Binbin Chen, Jian Weng, Zhuo Wei, Xin Li, Bo Qiu and Niekie Liu, “False Load Attack to Smart Meters by SynchronouslySwitching Power Circuits”, IEEE Transactions on Smart Grid, Vol. 10, No. 3, pp. 2641-2649, May 2019, DOI:10.1109/TSG.2018.2806896.

[25] Y. Sun, L. Lampe and V. W. S. Wong, “Smart Meter Privacy: Exploiting the Potential of Household Energy Storage Units”, IEEE Internet of ThingsJournal, Vol. 5, No. 1, pp. 69-78, Feb. 2018, DOI:10.1109/JIOT.2017.2771370.

[26] K. Ilango and George Fernandez. S, "Internet of Things (IoT) Based Automated Teller Machine Security System", Solid State Technology, Vol. 63, No. 3, pp. 816 - 825, 03-10-2020

[27] R. A. Akilesh, M. Kavya, M. Dhanavardhan, P. HarishKumar and Dr. K. Elango, "Energy Management In Micro Grid Using Distributed Generator", International Journal of Electrical Engineering and Technology, Vol. 12, No. 3, pp. 172-177, 12-03 2021.

[28] Geetha G. and Dr.K.Elango, "Online Adaptive Fault Classifier Module in High Voltage Transmission Line Using Fuzzy", Second IEEE National Conference on Emerging Trends in New and Renewable Energy Sources and Energy Management (NCET NRES EM- 2014), pp. 116-121, 16th DEC 2014