Securing Secondary Distribution with IoT-Based Smart Meters: Detection and Prevention of Power Theft

1st Sher Dali Khan
Faculty of Electrical and Electronic Engineering Technology
Universiti Teknikal Malaysia Melaka
Melaka, Malaysia
sherdalikhan2292@gmail.com

2nd Nurwahyu Alamsyah
Information Technology Department
Universitas Muhammadiyah Yogyakarta
Yogyakarta, Indonesia
nurwahyu.alamsyah@umy.ac.id

3rd Qazi Mazhar ul Haq
Department of Computer Science and Engineering and IBPI
Yuan Ze University
Taoyuan, Taiwan
qazi@saturn.yzu.edu.tw

4th Waqas Ahmad
Department of Electrical Engineering
University of Engineering & Technology
Mardan, Pakistan
Vickyahmad120@gmail.com

5th Naveed Mufti
Department of Telecommunication Engineering
University of Engineering & Technology
Mardan, Pakistan
naveed@uetmardan.edu.pk

6th Muhamad Amirul Haq,
Computer Science Department
Universitas Muhammadiyah Surabaya
Surabaya, Indonesia
amirulhaq@ft.um-surabaya.ac.id

2024 4th International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS) | 979-8-3503-7836-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICE3IS62977.2024.10775363

***Abstract*—Electrical energy distribution faces the significant issue of losses, with power theft being a main factor contributing to these losses. This difficulty is not limited to Pakistan but is also prevalent in several other nations worldwide. This study introduces a technique that utilizes smart meters to identify the approximate whereabouts of power theft. In addition to the detection of power theft, this study also presents a mechanism for the eradication of unauthorized users. The methodology used involves comparing the overall energy with the energy that is lawfully utilized. Wireless communication systems, such as Global System for Mobile Communications (GSM) and Network Repository Function (NRF), are used for communication between the meters.**

Keywords—Smart Meter, NRF based Smart Meter, Power Theft Prevention, Power Theft Elimination

I. Introduction

In recent years, contemporary technologies have transformed the global energy landscape to improve efficiency, reliability, and security. Smart grid technology relies on the Internet of Things (IoT), which has enabled several smart city innovations including object detection [1], notably in smart metering systems. Smart meters with IoT capabilities have revolutionized power usage monitoring and management. These systems focus on energy theft, which causes major economic and operational issues for utilities, particularly secondary distribution networks.

Utility companies worldwide struggle with electricity theft, or unlawful power use. Tampering with meters, creating unauthorized connections, and bypassing meters are examples. Energy theft costs billions of dollars annually, especially in poorer countries with poor infrastructure and enforcement, according to the World Bank [2]. Theft causes system inefficiencies, greater operating costs, and safety issues [3].

Real-time monitoring, data analysis, and automated anomaly reaction using IoT in smart metering systems may overcome these challenges. IoT smart meters may identify theft by sensing energy demand spikes, strange consumption patterns, or meter manipulation [4]. Data from sensors and communication equipment is analyzed by centralized management systems [5]. These capabilities help utilities detect and stop theft, reducing losses and improving power distribution network reliability [6]. Recent study shows that IoT-based smart metering solutions reduce power theft. Zheng et al. (2020) used machine learning techniques and IoT-enabled smart meters to detect theft-related usage trends [7]. After installing sophisticated metering networks, the authors noticed a significant drop in unaccounted-for power [8]. Sharma et al. (2019) examined IoT technologies in rural and urban locations and found that they may be readily extended and adapted to diverse operating settings [9].

IoT-based smart metering systems have great potential, but they must overcome numerous difficulties to be widely adopted and successful. Protecting data integrity and privacy is a problem. Hacks and unauthorized access to personal data are concerns when consumption data is collected and sent [10]. To safeguard client data and maintain trust in these technologies, robust encryption and secure communication protocols must be prioritized [11]. IoT-enabled smart meters need large initial infrastructure and technology expenditures, which may constrain utilities' finances, particularly in developing countries [12].

Smart metering systems using IoT require appropriate legislation. The creation and operation of these systems should be controlled to safeguard data, interoperate, and consumer rights [13]. Governments, utilities, and IT businesses must work on smart metering [14]. This study demonstrates IoT-based smart metering reduces secondary distribution network power theft. These systems' communication and technology are investigated. The essay addresses implementation challenges and solutions. Research and case studies demonstrate IoT improves smart meters. List of IoT-based smart metering sensor networks, communication technologies, and data analytics platforms. Machine learning, anomaly detection, and real-time monitoring will identify energy theft [15], [16]. The best techniques and experiences from global deployments will be highlighted [17], [18], [19], [20]. Government and regulatory issues are vital for these systems' successful implementation. IoT-based smart metering may improve power distribution network security, efficiency, and sustainability. Stopping power theft helps stabilize economies and build resilient energy infrastructure [21-25].

Four periods of the Industrial Revolution. The revolution started with new energy sources powering machinery. Introducing coal mining and steam-powered facilities were important [26]. Iron and steel industries advanced throughout the second revolution, which introduced mass production and electricity. Many enormous industrial plants with assembly lines were developed, generating new enterprises [27]. After the Third Revolution automated supply chains, computers and telephone connections were implemented [28]. The Fourth Industrial Revolution will be driven by advanced robotics, 5G, and IoT [29-31].

Data, processes, devices, and people are seamlessly interconnected by the IoT. IoT measures and analyzes behaviors to improve them. Big data is gathered and processed [31]. Healthcare, urban planning, construction, agriculture, water, and energy management may benefit from IoT [32]. This is done via real-time automated decision-making and evaluation systems. Meter reading, requiring utility company personnel visits, is inefficient and limited since energy meters cannot convey customer consumption (Figure 1). In urban or difficult terrain, this strategy demands a lot of physical work, time, and logistics. Manual reading mistakes may cause inaccurate invoicing, which annoys customers and costs energy providers [31].

Remotely monitored residential metering devices may address these issues. Remotely checking house meters is possible for utilities [32]. Modern wireless, cellular, and power line communication accomplish this. Using this technology simplifies meter reading, cutting operational costs and enhancing data accuracy [33]. The authors' domestic energy management system uses fog computing, an IoT-enabled smart plug, and a smart meter. The intelligent plug calculates RMS current, frequency, power factor, active power, and reactive power. To complete [34], develop and install an IoT-connected smart energy meter. Simple, affordable, and effective meter. Energy use by electrical devices will be recorded.

Remote control exceeds meter reading. These technologies may help utilities optimize energy consumption and save energy via demand-side management. Power companies have reduced grid overloads, regulated peak demands, and promoted energy sustainability [35]. By remotely changing parameters or load shedding. E-billing streamlines paper invoicing and facilitates remote control. Digital billing reduces paper waste and improves transparency [36]. More particular, [37] notes that users may quickly obtain billing information, examine energy usage trends, and make informed use decisions. Fixing this requires a very efficient pricing strategy [33]. Each user's smart meter needs an ECC. Connecting the communication structure and electrical grid with smart meters.

Computerized billing offers dynamic pricing. These models allow utility suppliers to adjust prices based on consumption, peak demand, and energy sources [39]. Customers may actively reduce energy usage by employing off-peak hours or energy-efficient practices. Electron billing benefits utilities and consumers by encouraging energy management cooperation [40].

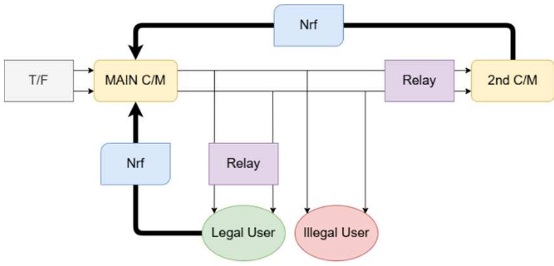

Fig. 1. Block Diagram of Proposed and Implemented Model

Remote control and automated billing enable data analytics and machine learning for utilities. Utility companies may detect consumption trends, inefficiencies, and targeted efforts to enhance service delivery and customer happiness by analyzing enormous datasets from meter readings and invoicing [34]. Analytical methods may improve operational efficiency and energy management [40], [41]. Machine learning may enhance IoT smart meter data gathering and processing [42-46]. Intelligent and sustainable energy management need these technologies [47-48].

Remote control and electronic invoicing systems provide unique issues. Data privacy, cybersecurity, and system resilience must be addressed thoroughly. To protect sensitive user data and system integrity, encryption, authentication, and access restrictions are essential [49].

II. System Design

We devised three smart meters, Two consumer smart meters (U/M) and Transformer smart check meters (T/F). In our designed system we will detect theft by installing a check meter after several connections, which will compare the output from transformer to the load. After theft detection it will send a message to the control room through wireless module NRF24101 to distribution transformer check meter shown in Figure 1.

The transformer check meter will show the total consumed units at that time. The transformer check meter will compare its output units with two consumers check meter. If the output of two consumer check meters is not equal to that of transformer output, then it will send message to control room that the theft is detected the flow chart of work is shown in Figure 2.

$$Power = V_{rms} \times I_{rms} \times cos(\emptyset) \qquad (1)$$

where,

$$V_{rms} = {V_o}/{\sqrt{2}} \text{ and } I_{rms} = {I_o}/{\sqrt{2}}$$

$$Energy = Power \times time \qquad (2)$$

A. Consumer's smart meter

The consumer's check meter can count the consumed units by the consumer. This meter also has the ability to send consumed units to the control room through NRF. And also, in case of theft detection the control room and user smart meter will communicate through NRF.

B. Distribution transformer check meter

The transformer check meter will show the total consumed units at that time. The transformer check meter will compare its output power with user's/consumers smart meters. If the output of two consumer check meter is not equal to that of transformer output, then it will send message to control room that the theft is detected.

III. MERITS OF PROPOSED METHODOLOGY

Smart Meter is the main building block of Smart Grid. Our modified Smart Meter devices give remote control over the individual user's energy. The updated meters will monitor user's energy meter to detect theft and then eliminate the theft, Illegal or unauthorized connection on secondary distribution line.

The proposed methodology enhances remote control and management of energy consumption through real-time monitoring and remote adjustments, providing significant advantages for users and utility companies. By enabling immediate detection and automated alerts for energy theft after the distribution transformer, the system ensures quick response and minimizes losses. This contributes to reduced operational costs and optimized energy usage, allowing users to anticipate bills and adjust consumption patterns for potential savings. Additionally, the methodology promotes user empowerment and transparency, fostering trust between consumers and providers, while supporting energy conservation and sustainability efforts. The primary objectives are to develop remote-controlled energy meters, implement theft detection mechanisms, enhance data monitoring and analysis, evaluate cost-benefit impacts, improve user-utility interaction, and promote sustainable energy practices, thereby demonstrating the system's effectiveness in improving energy management and reducing theft.

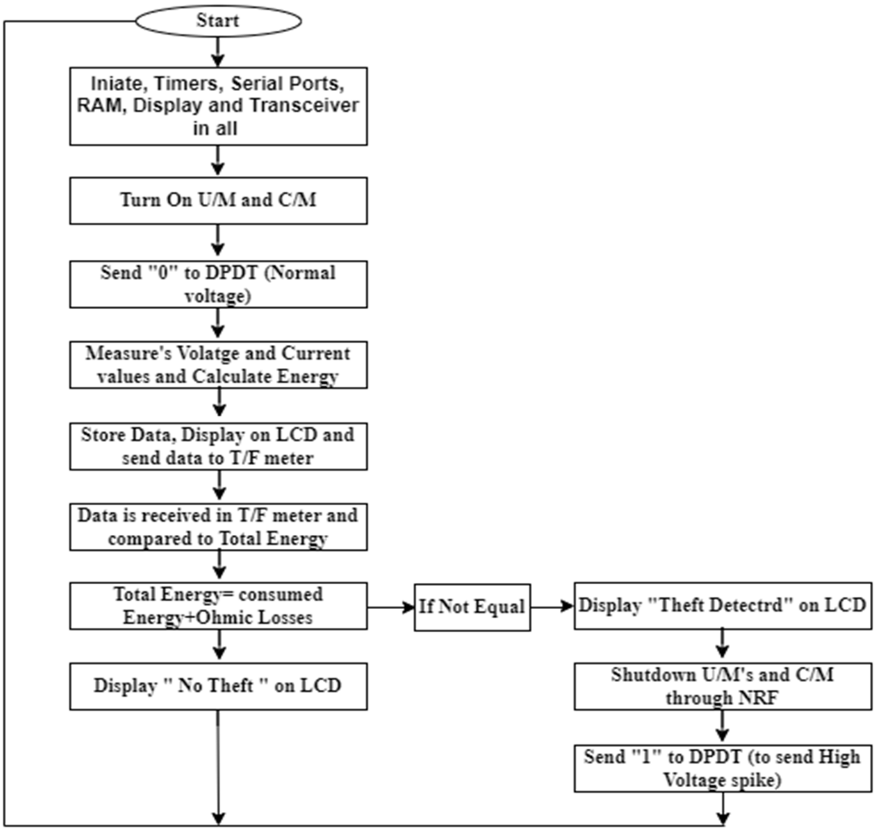

Fig. 2. Flow chart of Proposed Methodology

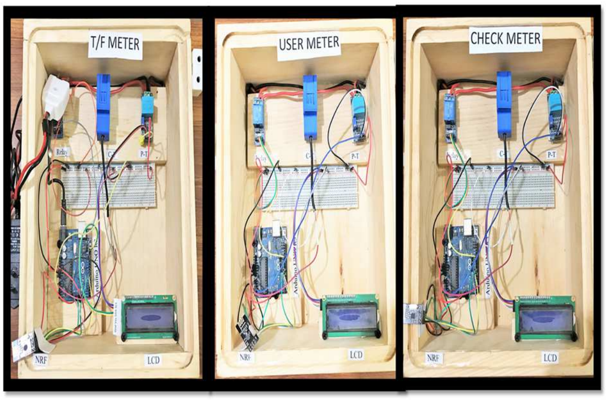

Fig. 3. Modified user's Smart meters and transformer check *meters*.

IV. RESULTS

In our designed system, theft will be detected by installing a check meter after several connections, which will compare the output of transformer to the sum of legal load. If the output of transformer is greater than the sum of all legal individual user's plus ohmic losses it means, there is illegal connection (theft) else no theft/illegal connection and the distribution is normal shown in Figure 5. In the case of theft detection, the transformer check meter (C/M) will send message to control room through wireless communication module (NRF24101) then after receiving message of theft/Illegal connection detection the control will send message to all legal users to switch off. After switching off all legal users (U/M), the control room will send "1" to DPDT to send High Voltage Spike to burn out/eliminate the illegal connection.

A. *Theft Detection Scenario*

Detection of power theft is done by the synchronization of these check meters. As discussed earlier the transformer check meter will show the total consumed units at that time and the NRF meter installed is shown in Figure 4. Therefore, when someone is trying to power theft using a wire, the extra units consumed in the form of that will be shown on transformer check meter after comparison with local consumers check meter. These readings will be sent out to the control room through NRF. Moreover, with the help of these meters, we cannot only easily detect the illegal and consumed units but can also the approximate location of power theft.

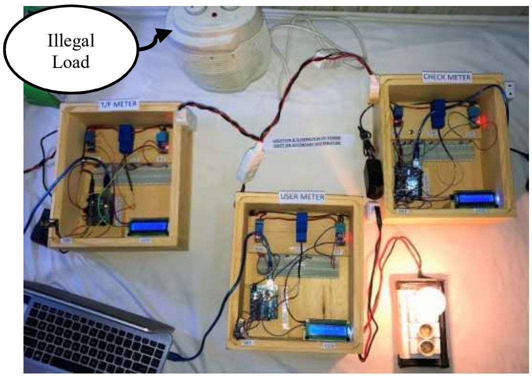

Fig. 4. Designed prototype

B. *Elimination of electricity theft on Secondary Distribution*

When our designed model/system locates the theft or illegal connection on secondary distribution line then from control room/ T/F meter the legal user smart meters will off, and then High voltage spike will generate by the T/F meter. It will eliminate the illegal connections/theft on distribution line shown in Figure 6.

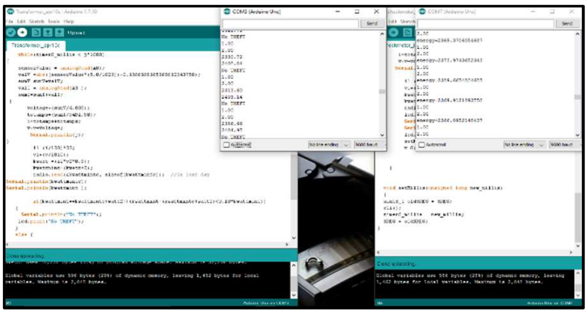

Fig. 5. No Theft Detection Scenario.

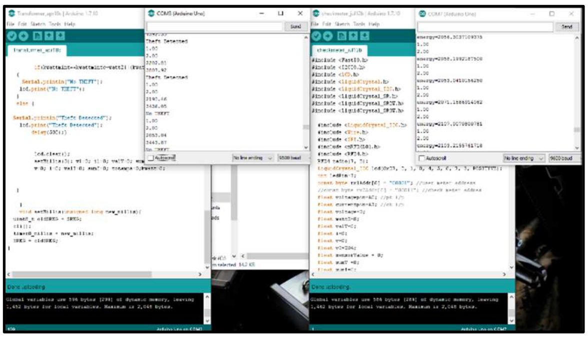

Fig. 6. Theft Detection Scenario Snapshot

V. CONCLUSIONS

With the advancement of technology, the method of electricity theft is getting advanced. Consumers are discovering fresh ways and techniques to tamper their meters. That's why the present metering system (Analog or simple digital meters) cannot fit this era especially in Pakistan. To deal with such advanced criminal's smart grid system is compulsory. The proposed mechanism interconnects the whole distribution system resulting in minimizing illegal consumption of electric energy. Besides theft detection, this article also provides an approach to eliminate the illegal consumers of electricity.

TABLE I. COMPARISON KEY FEATURES OF OUR MODIFIED SMART METER WITH OTHER METERS

Key Features	Traditional Analogue Meter	Digital Energy meter	Our Modified Smart Energy Meter
Remote Control	×	×	✓
Theft Detection	×	×	✓
Theft Elimination	×	×	✓
Distribution Transformer Over-load Protection	×	×	✓

REFERENCES

[1] Q. M. Ul Haq et al., "An Incremental Learning of YOLOv3 Without Catastrophic Forgetting for Smart City Applications," IEEE Consum. Electron. Mag., vol. 11, no. 5, pp. 56–63, 2022, doi: 10.1109/MCE.2021.3096376.

[2] A. G. Keane et al., "The impact of electricity theft on power system operation and planning," IEEE Transactions on Power Systems, vol. 34, no. 4, pp. 2959-2970, July 2019.

[3] S. H. Horng et al., "A novel smart meter system for power grid theft prevention," IEEE Transactions on Smart Grid, vol. 6, no. 1, pp. 142-152, Jan. 2015.

[4] R. Sharma, A. S. Reddy, and S. Singh, "IoT-based smart energy meter: An innovative solution for energy management and theft detection," International Journal of Engineering and Advanced Technology (IJEAT), vol. 8, no. 6, pp. 2398-2403, Aug. 2019.

[5] M. A. Rahman and M. I. Islam, "Cybersecurity issues in IoT-based smart metering," IEEE Internet of Things Journal, vol. 7, no. 11, pp. 11023-11033, Nov. 2020.

[6] B. T. Ingole, D. P. Kumar, and S. P. Gawande, "Policy frameworks for IoT-based smart grid systems: A comprehensive review," IEEE Access, vol. 8, pp. 175635-175649, Sep. 2020.

[7] J. Zheng, D. W. Gao, and L. Lin, "Smart meters in smart grid: An overview," IEEE Transactions on Industrial Informatics, vol. 15, no. 2, pp. 1193-1204, Feb. 2020.

[8] M. E. Kargarian et al., "Toward distributed/decentralized DC optimal power flow implementation in future electric power systems," IEEE Transactions on Smart Grid, vol. 9, no. 4, pp. 2574-2587, Jul. 2018.

[9] P. P. Ray, "A survey on Internet of Things architectures," Journal of King Saud University - Computer and Information Sciences, vol. 30, no. 3, pp. 291-319, Jul. 2018.

[10] H. Yan, K. Ma, "Machine learning for anomaly detection in IoT-based smart grid," IEEE Transactions on Industrial Informatics, vol. 15, no. 8, pp. 4757-4765, Aug. 2019.

[11] J. Q. Sun et al., "IoT-based smart grid: Current applications and future prospects," IEEE Internet of Things Journal, vol. 7, no. 4, pp. 3189-3202, Apr. 2020.

[12] F. Benzi, N. Anglani, E. Bassi, and L. Frosini, "Electricity smart meters interfacing the households," IEEE Transactions on Industrial Electronics, vol. 58, no. 10, pp. 4487-4494, Oct. 2018.

[13] A. Alahakoon and X. Yu, "Smart electricity meter data intelligence for future energy systems: A survey," IEEE Transactions on Industrial Informatics, vol. 12, no. 1, pp. 425-436, Feb. 2018.

[14] M. Aman, M. S. Ghazvini, Y. Simmhan, and R. Buyya, "An efficient and energy-aware computing model for smart homes," IEEE Transactions on Industrial Informatics, vol. 13, no. 6, pp. 2884-2894, Dec. 2019.

[15] D. Gupta, N. Jain, and P. Agrawal, "Machine learning applications for cybersecurity in IoT-based smart grid networks," Journal of Network and Computer Applications, vol. 163, pp. 102635, Jan. 2020.

[16] G. N. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, "IoT middleware: A survey on issues and enabling technologies," IEEE Internet of Things Journal, vol. 4, no. 1, pp. 1-20, Feb. 2017.

[17] R. A. Akilimali, P. R. Kumar, "The future of IoT-based smart grids: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3653-3675, Jul. 2018.

[18] A. A. Radwan, A. M. F. Raafat, "IoT-based power theft detection in smart grids," IEEE Transactions on Industrial Electronics, vol. 66, no. 12, pp. 9627-9636, Dec. 2019.

[19] P. Kulkarni, P. Kulkarni, "AI-driven IoT-based smart meter architecture for detection of non-technical losses," IEEE Transactions on Smart Grid, vol. 10, no. 3, pp. 2916-2925, May 2019.

[20] J. C. Raj, R. G. Mekala, "Analysis of IoT-based smart meters for electricity theft detection," IEEE Transactions on Industrial Electronics, vol. 66, no. 12, pp. 9616-9626, Dec. 2019.

[21] M. Faisal, S. M. Riazul Islam, "Securing IoT-based smart meters in the smart grid: A deep learning approach," IEEE Transactions on Smart Grid, vol. 11, no. 3, pp. 2075-2086, May 2020.

[22] F. Hussain, M. Abolhasan, J. W. Mark, "A survey on security and privacy issues of smart meters in smart grids," IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 282-298, 2018.

[23] J. Qi, J. Zhang, "A comprehensive review on cyber-physical smart grid testbeds," IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1796-1823, 2017.

[24] A. Moreno-Muñoz et al., "Integration of renewables in the smart grid: Technologies and challenges," IEEE Transactions on Smart Grid, vol. 10, no. 2, pp. 1051-1064, Mar. 2019.

[25] L. D. Xu, W. He, and S. Li, "Internet of Things in industries: A survey," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233-2243, Nov. 2018.

[26] A. Ravasoo, "Interaction of bursts in exponentially gradedmaterials characterized by parametric plots," *Wave Motion*, vol. 51, no. 5, pp. 758–767, 2014, doi: 10.1016/j.wavemoti.2014.01.006.

[27] M. C. JENSEN, "The Modern Industrial Revolution, Exit, and the Failure of Internal Control Systems," *J. Finance*, vol. 48, no. 3, pp. 831–880, 1993, doi: 10.1111/j.1540-6261.1993.tb04022.x.

[28] S. K. Datta and C. Bonnet, "MEC and IoT Based Automatic Agent Reconfiguration in Industry 4.0," *Int. Symp. Adv. Networks Telecommun. Syst. ANTS*, vol. 2018-December, pp. 1–5, 2018, doi: 10.1109/ANTS.2018.8710126.

[29] F. Shrouf, J. Ordieres, and G. Miragliotta, "Smart factories in Industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm," *IEEE Int. Conf. Ind. Eng. Eng. Manag.*, vol. 2015-January, pp. 697–701, 2014, doi: 10.1109/IEEM.2014.7058728.

[30] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," *Wirel. Pers. Commun.*, vol. 58, no. 1, pp. 49–69, 2011, doi: 10.1007/s11277-011-0288-5.

[31] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. Shen, "Energy-theft detection issues for advanced metering infrastructure in smart grid," *Tsinghua Sci. Technol.*, vol. 19, no. 2, pp. 105–120, 2014, doi: 10.1109/TST.2014.6787363.

[32] R. Podmore and M. R. Robinson, "The role of simulators for smart grid development," *IEEE Trans. Smart Grid*, vol. 1, no. 2, pp. 205–212, 2010, doi: 10.1109/TSG.2010.2055905.

[33] H. Mortaji, S. H. Ow, M. Moghavvemi, and H. A. F. Almurib, "Load Shedding and Smart-Direct Load Control Using Internet of Things in Smart Grid Demand Response Management," *IEEE Trans. Ind. Appl.*, vol. 53, no. 6, pp. 5155–5163, 2017, doi: 10.1109/TIA.2017.2740832.

[34] A. N. F. Ali, M. F. Sulaima, I. A. W. A. Razak, A. F. A. Kadir, and H. Mokhlis, "Artificial Intelligence Application in Demand Response: Advantages, Issues, Status, and Challenges," *IEEE Access*, vol. 11, no. December 2022, pp. 16907–16922, 2023, doi: 10.1109/ACCESS.2023.3237737

[35] I. Ben Dhaou, "Design and Implementation of an Internet-of-Things-Enabled Smart Meter and Smart Plug for Home-Energy-Management System," *Electron.*, vol. 12, no. 19, pp. 1–20, 2023, doi: 10.3390/electronics12194041.

[36] S. Muralidhara, N. Hegde, and R. PM, "An internet of things-based smart energy meter for monitoring device-level consumption of energy," *Comput. Electr. Eng.*, vol. 87, p. 106772, 2020, doi:10.1016/j. compeleceng. 2020.106772.

[37] N. Javaid *et al.*, "Demand side management in nearly zero energy buildings using heuristic optimizations," *Energies*, vol. 10, no. 8, pp. 1–29, 2017, doi: 10.3390/en10081131.

[38] K. Hopf, M. Sodenkamp, and T. Staake, "Enhancing energy efficiency in the residential sector with smart meter data analytics," *Electron. Mark.*, vol. 28, no. 4, pp. 453–473, 2018, doi: 10.1007/s12525-018-0290-9.

[39] P. Samadi, H. Mohsenian-Rad, R. Schober, and V. W. S. Wong, "Advanced demand side management for the future smart grid using mechanism design," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1170–1180, 2012, doi: 10.1109/TSG.2012.2203341.

[40] M. A. Raza, M. M. Aman, A. G. Abro, M. A. Tunio, K. L. Khatri, and M. Shahid, "Challenges and potentials of implementing a smart grid for Pakistan's electric network," *Energy Strateg. Rev.*, vol. 43, no. January, p. 100941, 2022, doi: 10.1016/j.esr.2022.100941.

[41] D. Moscovitz, Z. Zhao, L. Du, and X. Fan, "Semi-Supervised, Non-Intrusive Disaggregation of Nodal Load Profiles With Significant Behind-the-Meter Solar Generation," *IEEE Trans. Power Syst.*, vol. 39, no. 3, pp. 4852–4864, 2024, doi: 10.1109/TPWRS.2023.3334995.

[42] H. P. Josyula, L. T. Reddi, S. Parate, and A. Rajagopal, "A Review on Security and Privacy Considerations in Programmable Payments," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 9, pp. 256–263, 2024.

[43] S. Karam, S. J. Ruan, and Q. M. Ul Haq, "Task Incremental Learning with Static Memory for Audio Classification Without Catastrophic Interference," *IEEE Consum. Electron. Mag.*, vol. 11, no. 5, pp. 101–108, 2022, doi: 10.1109/MCE.2022.3145724.

[44] L. Yao, B. Y. Lin, Q. M. Ul Haq, and I. Ul Islam, "Unsupervised Cross-Domain Adaptation through Mutual Mean Learning and GANs for Person Re-identification," *3rd IEEE Int. Conf. Artif. Intell. ICAI 2023*, no. February, pp. 122–128, 2023, doi: 10.1109/ICAI58407.2023.10136664.

[45] Q. M. Ul Haq *et al.*, "An Incremental Learning of YOLOv3 Without Catastrophic Forgetting for Smart City Applications," *IEEE Consum. Electron. Mag.*, vol. 11, no. 5, pp. 56–63, 2022, doi: 10.1109/MCE.2021.3096376.

[46] Q. M. ul Haq, L. Yao, W. Rahmaniar, Fawad, and F. Islam, "A Hybrid Hand-Crafted and Deep Neural Spatio-Temporal EEG Features Clustering Framework for Precise Emotional Status Recognition," *Sensors*, vol. 22, no. 14, 2022, doi: 10.3390/s22145158.

[47] Q. M. ul Haq, C. H. Lin, S. J. Ruan, and D. Gregor, "An edge-aware based adaptive multi-feature set extraction for stereo matching of binocular images," *J. Ambient Intell. Humaniz. Comput.*, vol. 13, no. 4, pp. 1953–1967, 2022, doi: 10.1007/s12652-021-02958-8.

[48] Q. M. ul Haq *et al.*, "Identification of Software Bugs by Analyzing Natural Language-Based Requirements Using Optimized Deep Learning Features," *Comput. Mater. Contin.*,

[49] Naim Abdullah and Ghouri Arsalan, "Exploring the Role of Cybersecurity Measures (Encryption, Firewalls, andAuthentication Protocols) in Preventing Cyber-attacks on E-commercePlatforms," *Int. J. Ebus. eGovernment Stud.*, no. November, pp. 444–468, 2023, doi: 10.34109/ijebeg.2023150120.