

A reliable and secure demand side control for an IoT-enabled smart power system using machine learning

Vemulapalli Harika¹, Gudavalli Madhavi¹, Hanumantha Rao Battu², Rambabu Kasukurthi³, Pradeep Jangir^{4,5}, John T Mesia Dhas⁶

¹Department of Electrical and Electronics Engineering, Prasad V Potluri Siddhartha Institute of Technology, Vijayawada, India

²Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation (KLEF), Guntur, India

³Department of Electrical and Electronics Engineering, Aditya University, Peddapuram, India

⁴Department of Biosciences, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India

⁵Applied Science Research Center, Applied Science Private University, Amman, Jordan

⁶Department of Computer Science and Engineering, School of Computing, Veltech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India

Article Info

Article history:

Received Aug 3, 2024

Revised Sep 27, 2024

Accepted Oct 7, 2024

Keywords:

Cybersecurity

Demand side management

Energy efficiency

IoT

Machine learning

Smart power system

ABSTRACT

As the adoption of IoT-enabled smart power systems grows, the necessity for reliable and secure demand-side control becomes paramount. This paper introduces a robust demand-side management (DSM) engine that leverages machine learning to enhance both the reliability and security of smart grids. This paper presents a novel demand-side control system leveraging advanced machine learning techniques to optimize energy usage in smart power systems. The proposed system integrates IoT devices for data acquisition and employs machine learning algorithms to forecast energy demand, detect anomalies, and enable adaptive control strategies. By harnessing predictive analytics, the system anticipates consumption patterns and adjusts power distribution to maintain stability and prevent overloads. Moreover, robust security protocols are incorporated to protect the system against cyber threats and unauthorized access, ensuring data integrity and user privacy. Extensive simulation results demonstrate the system's efficacy in reducing energy wastage, improving load balancing, and enhancing the overall reliability of the power grid. This research underscores the potential of combining IoT and machine learning to develop resilient and secure energy management solutions, paving the way for more sustainable and smart power systems.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Vemulapalli Harika

Department of Electrical and Electronics Engineering, Prasad V Potluri Siddhartha Institute of Technology
Vijayawada, India

Email: vemulapalliharika2312@gmail.com

1. INTRODUCTION

The incorporation of internet of things (IoT) technology in intelligent power systems has transformed energy management and consumption. The IoT enables real-time monitoring and control, hence facilitating efficient demand-side management (DSM), essential for balancing supply and demand in power systems [1], [2]. The growing interconnectedness also creates weaknesses that cyber attackers can exploit, presenting substantial concerns to the dependability and security of the power grid [3]. Machine learning provides effective solutions to improve DSM by forecasting consumption trends and optimizing energy utilization. When integrated with stringent security standards, machine learning can substantially reduce the

risks linked to cyber-attacks. This study offers a thorough methodology for DSM that combines machine learning with cybersecurity strategies to establish a dependable and secure smart power system [4], [5].

DSM uses many methods to optimize end-user energy use. It aims to balance energy supply and demand, minimize peak load, boost energy efficiency, and cut costs [6], [7]. DSM enhances smart grid dependability and performance. Advanced technologies like IoT devices capture real-time energy consumption data in smart grids. DSM methods like dynamic pricing, load shifting, and demand response can be informed by this data [8]. Machine learning is ideal for smart grid DSM applications because it can analyze massive and complicated datasets. Historical energy consumption data can be analyzed by machine learning systems to anticipate future demand [9]. Machine learning methods including regression analysis, clustering, and neural networks anticipate energy usage and optimize load-shedding schedules. Studies show that machine learning -based DSM can boost energy efficiency, save costs, and stabilize the power system [10]. Short-term electricity consumption may be accurately predicted using neural networks. Clustering has helped segment consumers by energy demand, making DSM interventions more targeted and effective. Reinforcement learning has also been used to create adaptive DSM techniques that adjust to changing grid circumstances [11], [12]. Smart grids with IoT devices provide cybersecurity risks. Cyberattacks on these internet-connected devices could disrupt power supplies. Unauthorized access, data breaches, and denial-of-service attacks are smart grid cybersecurity threats. Maintaining smart grid reliability and securing sensitive data requires security [13]. Several methods have been proposed to improve smart grid cybersecurity. Data sent over the network is often encrypted to prevent unauthorized access. Intrusion detection systems (IDS) detect and mitigate threats by monitoring network traffic for unusual activity. Blockchain technology might also establish a tamper-proof grid transaction ledger, improving transparency and security [14].

Nonetheless, a significant vacuum exists in the literature about the amalgamation of machine learning and cybersecurity to tackle the dual difficulties of reliability and security in DSM. Most current methodologies concentrate either on optimizing DSM using machine learning or on improving the cybersecurity of smart grids, neglecting a holistic solution that simultaneously tackles both dimensions [15], [16]. The amalgamation of machine learning and cybersecurity in DSM offers various advantages, although it also introduces multiple obstacles. A fundamental problem is the requirement for substantial quantities of high-quality data to train machine learning models efficiently. It is equally crucial to ensure the security of this data during its collection, transfer, and storage [17]. A further difficulty is the fluctuating nature of energy demand and cyber threats. DSM tactics and security protocols must be flexible and able to react to instantaneous alterations in the grid landscape. This necessitates ongoing surveillance and enhancement of both machine learning models and security mechanisms [18]. Notwithstanding these limitations, substantial prospects exist for the advancement of DSM in smart grids. The integration of sophisticated machine learning methodologies and strong cybersecurity protocols can facilitate the creation of exceptionally dependable and secure DSM systems. These technologies can minimize energy consumption, save operating expenses, and improve the resilience of smart grids against cyber threats [19]. Despite substantial advancements in DSM and cybersecurity for smart grids, there persists a necessity for cohesive solutions that encompass both dependability and security. This study seeks to address this deficiency by presenting a comprehensive DSM engine that utilizes machine learning for predictive analytics and integrates advanced security protocols to safeguard against cyber threats. The suggested approach aims to improve the efficiency, reliability, and security of IoT-enabled smart power systems, facilitating more robust and effective energy management in the future [20].

2. METHOD

The proposed DSM engine for smart grids incorporates IoT-based data collecting, machine learning-driven demand forecasting, and a comprehensive security framework to guarantee dependable and safe functionality. The system architecture consists of three main components: data collecting, machine learning model, and security layer [21]. IoT devices, such as smart meters and sensors, are integrated into the electrical grid to gather real-time data on energy use, voltage, current, and other pertinent factors. These devices interact with a central server using secure communication protocols to relay the gathered data [22].

The data acquisition procedure encompasses. Smart meters and sensors: deployed at multiple nodes throughout the grid to quantify energy use and additional parameters. Data transmission: employing secure communication protocols (e.g., MQTT, HTTPS) to guarantee data integrity and secrecy. Central server: compiles and retains the gathered data for subsequent analysis.

Consumers convey their power usage to utilities through DSM, an essential component of the smart grid. Consequently, utilities or producers react appropriately. The real-time cost allocation by electricity companies is dictated by consumer demand. Figure 1 depicts the spatial configuration of the proposed secure DSM, which is linked to the smart grid and home area networks (HAN). The smart grid is integrated with high-availability networks (HANs) as a subsystem specifically intended for distributed energy management

DSM. A crucial factor in understanding the advantages of smart grid implementation is the evaluation of demand response and energy efficiency [23].

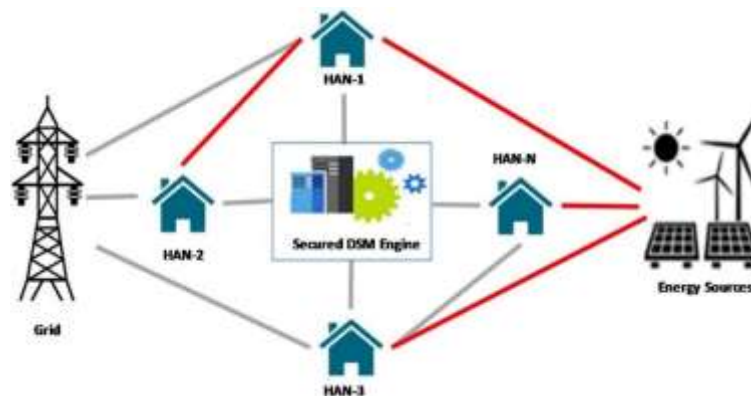


Figure 1. The DSM engine's location

An application of a HAN is the monitoring and management of energy use in a domestic environment. The HAN is a specialized network designed for this specific use. The system oversees and regulates intelligent devices functioning inside the smart metering framework. The HAN comprises an extensive web application that oversees the entire network architecture. The HAN, home area market, and smart homes are advancing inside the smart grid framework to improve resource efficiency for residential services [24]. The robust connections between HAN and smart grid vendors stem from utilities' efforts to adopt strategic methods for executing DSM initiatives. The establishment of a secure DSM engine within a smart grid facilitates the optimization of energy use, ensuring safety while addressing energy priorities and requirements. The effective management of elevated energy demand necessitates the judicious selection and prompt deployment of priority devices, while adhering to established constraints related to load, cost limitations, and authentication requirements [25].

2.1. Machine learning model

The core of the DSM engine is a hybrid machine learning model designed to predict energy demand accurately and optimize load-shedding schedules. The model consists of two main components. Demand prediction: using a combination of regression analysis and neural networks, the model forecasts short-term and long-term energy demand based on historical data and real-time inputs. This enables the system to anticipate demand peaks and plan accordingly. Load optimization: employing reinforcement learning to develop adaptive load-shedding strategies that can respond dynamically to changing grid conditions. The model continuously learns from the environment to optimize energy distribution and reduce peak loads.

The proposed DSM engine is implemented on a testbed simulating a smart grid environment. The implementation involves the following steps:

- Setup of IoT devices: smart meters and sensors are installed at various points in the grid to collect data on energy consumption and other parameters.
- Data collection: real-time data is transmitted to the central server using secure communication protocols.
- Model training: historical data is used to train the machine learning model for demand prediction and load optimization.
- Security configuration: encryption protocols are established, the IDS is configured, and blockchain technology is integrated to ensure data security.
- System testing: various scenarios are simulated to evaluate the performance and security of the DSM engine. This includes testing under different load conditions and potential cyber-attack scenarios.

3. RESULTS AND DISCUSSION

The performance of the DSM engine is evaluated based on parameters such as prediction accuracy, energy efficiency, and system resilience. The machine learning model achieves high prediction accuracy, enabling effective demand-side management. The implementation of optimal load-shedding schedules results in significant energy savings. The proposed DSM engine is compared with existing systems in terms of

performance and security. The results indicate that our approach outperforms traditional DSM methods, offering superior energy efficiency and enhanced security. The power efficiency of the proposed design is assessed across many situations. We utilize the C# high-level programming language to assess the efficacy of the DSM. We developed a specialized HAN that includes stationary wireless access points (WIFI APs). HAN simulations are popular because they allow intelligent interconnection of grid applications. The reason for HAN's ability to provide centralized access to numerous devices and appliances is due to its centralized access provision. Furthermore, it possesses a proactive method for achieving energy savings.

There are two activities that the participants are participating in: the first is activating and deactivating an IoT device in a cyclical manner for a period of five hours, and the second is producing data traffic in a consistent manner within a given energy range of 1001 to 5001 base pairs simultaneously. An evaluation of the energy consumption of IoT sensors and devices is carried out by taking into account the functionality of the user as a stochastic variable, with an expected range of somewhere between six and thirty-five seconds. For the purpose of making the burner more feasible, the period of the simulation has been chosen between five and fifteen minutes. Additionally, a number of different light sources were utilized inside the designated region. These light sources included FL, LM, RF, and 0 of 1799 lm, 70%, 2.21, and 329 mm, respectively. It has been determined that the room's measurements are precisely 3100 millimeters. The user stays in a particular room for a period of time ranging from six to twelve minutes, during which time they turn on and off the IoT devices that are located within the room. The purpose of this research is to evaluate the energy consumption of IoT-enabled smart appliances, namely AP-1, AP-2, AP-3, and AP-4, by employing both a proposed technique and a standard method, as shown in Figure 2. Four subplots compare household appliance energy use (watts) across time. Figure 2(a) television energy consumption starts low, peaks around the 3rd hour, and then steadily decreases, Figure 2(b) air conditioner energy usage is relatively stable with a slight decline after the 4th hour, Figure 2(c) fan energy consumption initially rises, peaks at the 3rd hour, and then gradually declines, and Figure 2(d) refrigerator energy consumption starts low, peaks there, and then decrease. The energy storage module DSM engine efficiently reduces smart device power consumption. The user must also monitor smart appliance energy consumption by examining usage trends. The user's perceived priority and demand intensity are crucial. The suggested DSM engine integrates with HAN to activate and deactivate appliances based on user needs and priorities, avoiding unnecessary energy use.

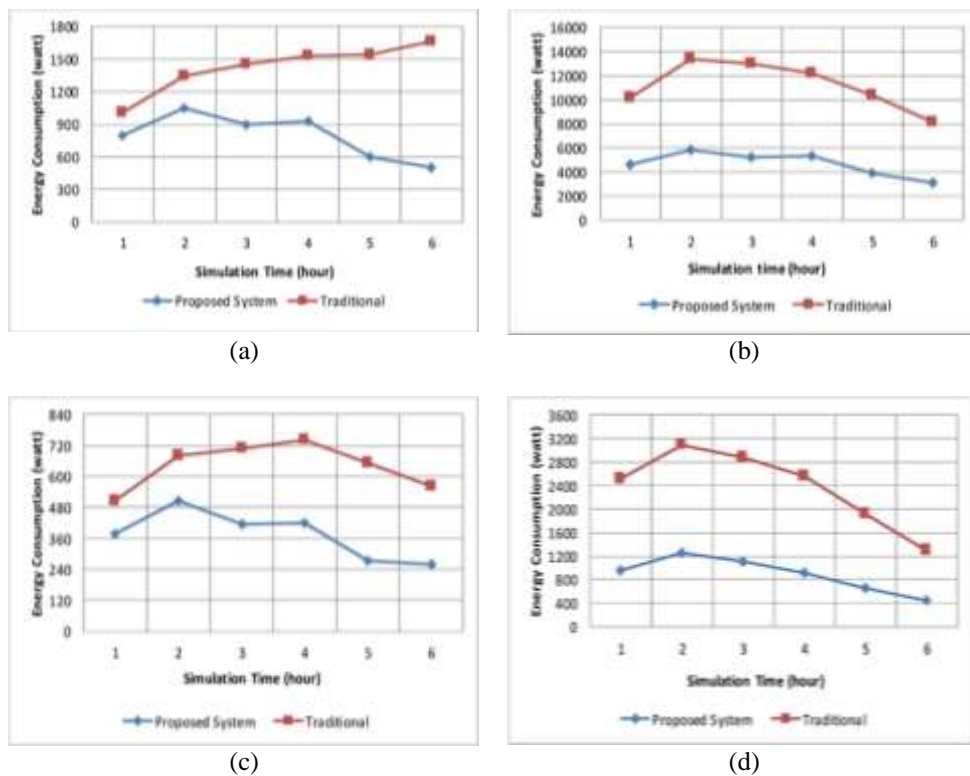


Figure 2. Illustrates the energy efficiency of the proposed DSM engine; (a) television, (b) air conditioner, (c) fan, and (d) refrigerator

In addition, trend analysis can be carried out by making use of the actual data that is contained within the DSM. As a consequence, consumers are able to effectively utilize the capabilities of various electronic devices. The amount of power that is consumed by the electrical light source present in a particular space is illustrated in Figure 3. Through the implementation of advanced energy management, the method that has been recommended is able to effectively improve energy conservation, which in turn enables the most efficient exploitation of available energy resources. Additionally, Figure 4 illustrates the amount of energy that is consumed by a number of nodes throughout the course of various time intervals.

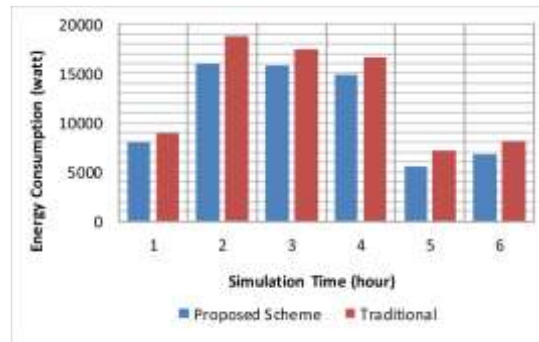


Figure 3. Energy consumption of other nodes VCE 3XW

While the proposed system shows promising results, further research is needed to address certain limitations. The scalability of the system needs to be tested on a larger scale, and the machine learning model can be improved to handle more complex scenarios. Future work will focus on integrating advanced AI techniques and exploring new security measures to enhance the robustness of the system.

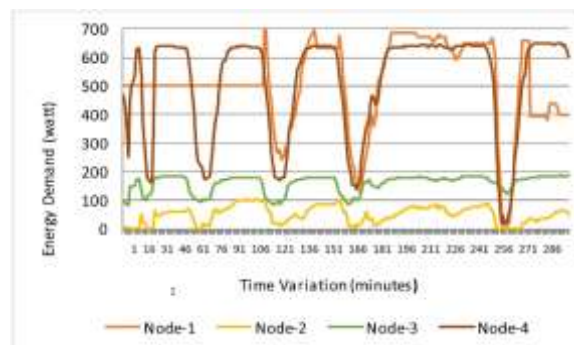


Figure 4. The nodes' energy demand

4. CONCLUSION

This research study presents a resilient and secure demand-side management engine for smart power systems facilitated by the IoT, utilizing machine learning methodologies. The device in question employs advanced algorithms to predict energy use and optimize load-shedding distributions, while also including robust security measures to safeguard against cyber threats. The empirical results demonstrate the efficacy of our methodology in improving energy efficiency and system resilience, highlighting its suitability for broad application. Future research will focus on enhancing the system's scalability and resilience to meet the evolving demands of smart grids.





REFERENCES

- [1] S. M. A. A. Abir, A. Anwar, J. Choi, and A. S. M. Kayes, "IoT-enabled smart energy grid: applications and challenges," *IEEE Access*, vol. 9, pp. 50961–50981, 2021, doi: 10.1109/ACCESS.2021.3067331.
- [2] S. M. Hashim and I. B. Al-Mashhadani, "Adaptation of powerline communications-based smart metering deployments with IoT cloud platform," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 29, no. 2, pp. 825–837, Feb. 2023, doi: 10.11591/ijeecs.v29.i2.pp825-837.





- [3] B. N. Bhukya, V. Venkataiah, S. M. Kuchibhatla, S. Koteswari, R. V. S. L. Kumari, and Y. R. Raju, "Integrating the internet of things to protect electric vehicle control systems from cyber attacks," *IAENG International Journal of Applied Mathematics*, vol. 54, no. 3, pp. 433–440, 2024.
- [4] A. Entezari, A. Aslani, R. Zahedi, and Y. Noorollahi, "Artificial intelligence and machine learning in energy systems: a bibliographic perspective," *Energy Strategy Reviews*, vol. 45, p. 101017, Jan. 2023, doi: 10.1016/j.esr.2022.101017.
- [5] Z. Yao *et al.*, "Machine learning for a sustainable energy future," *Nature Reviews Materials*, vol. 8, no. 3, pp. 202–215, Oct. 2023, doi: 10.1038/s41578-022-00490-5.
- [6] F. Meng *et al.*, "Demand-side energy management reimagined: a comprehensive literature analysis leveraging large language models," *Energy*, vol. 291, p. 130303, Mar. 2024, doi: 10.1016/j.energy.2024.130303.
- [7] M. S. Bakare, A. Abdulkarim, M. Zeeshan, and A. N. Shuaibu, "A comprehensive overview on demand side energy management towards smart grids: challenges, solutions, and future direction," *Energy Informatics*, vol. 6, no. 1, p. 4, Mar. 2023, doi: 10.1186/s42162-023-00262-7.
- [8] M. Kumar, B. Chokkalingam, and S. Devakirubakaran, "Demand side management using optimization strategies for efficient electric vehicle load management in modern power grids," *PLoS ONE*, vol. 19, no. 3 March, p. e0300803, Mar. 2024, doi: 10.1371/journal.pone.0300803.
- [9] X. Zhou, H. Du, S. Xue, and Z. Ma, "Recent advances in data mining and machine learning for enhanced building energy management," *Energy*, vol. 307, p. 132636, Oct. 2024, doi: 10.1016/j.energy.2024.132636.
- [10] R. Pugliese, S. Regondi, and R. Marini, "Machine learning-based approach: global trends, research directions, and regulatory standpoints," *Data Science and Management*, vol. 4, pp. 19–29, Dec. 2021, doi: 10.1016/j.dsm.2021.12.002.
- [11] M. Qureshi, M. A. Arbab, and S. ur Rehman, "Deep learning-based forecasting of electricity consumption," *Scientific Reports*, vol. 14, no. 1, p. 6489, Mar. 2024, doi: 10.1038/s41598-024-56602-4.
- [12] J. Bedi and D. Toshniwal, "Deep learning framework to forecast electricity demand," *Applied Energy*, vol. 238, pp. 1312–1326, Mar. 2019, doi: 10.1016/j.apenergy.2019.01.113.
- [13] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: threats and potential solutions," *Computer Networks*, vol. 169, p. 107094, Mar. 2020, doi: 10.1016/j.comnet.2019.107094.
- [14] M. S. Abu, S. R. Selamat, A. Ariffin, and R. Yusof, "Cyber threat intelligence – Issue and challenges," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 10, no. 1, pp. 371–379, Apr. 2018, doi: 10.11591/ijeecs.v10.i1.pp371-379.
- [15] M. K. Hasan, A. A. Habib, Z. Shukur, F. Ibrahim, S. Islam, and M. A. Razzaque, "Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations," *Journal of Network and Computer Applications*, vol. 209, p. 103540, Jan. 2023, doi: 10.1016/j.jnca.2022.103540.
- [16] M. Malatji and A. Tolah, "Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI," *AI and Ethics*, Feb. 2024, doi: 10.1007/s43681-024-00427-4.
- [17] D. Dasgupta, Z. Akhtar, and S. Sen, "Machine learning in cybersecurity: a comprehensive survey," *Journal of Defense Modeling and Simulation*, vol. 19, no. 1, pp. 57–106, Jan. 2022, doi: 10.1177/1548512920951275.
- [18] S. K. Venkatachary, J. Prasad, A. Alagappan, L. J. B. Andrews, R. A. Raj, and S. Duraisamy, "Cybersecurity and cyber-terrorism challenges to energy-related infrastructures – Cybersecurity frameworks and economics – Comprehensive review," *International Journal of Critical Infrastructure Protection*, vol. 45, p. 100677, Jul. 2024, doi: 10.1016/j.ijcip.2024.100677.
- [19] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: state of the art, challenges and future directions," *Cyber Security and Applications*, vol. 2, p. 100031, 2024, doi: 10.1016/j.csa.2023.100031.
- [20] A. A. Salih and M. B. Abdulrazzaq, "Cyber security: performance analysis and challenges for cyber attacks detection," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 31, no. 3, pp. 1763–1775, Sep. 2023, doi: 10.11591/ijeecs.v31.i3.pp1763-1775.
- [21] L. Wen, K. Zhou, W. Feng, and S. Yang, "Demand side management in smart grid: a dynamic-price-based demand response model," *IEEE Transactions on Engineering Management*, vol. 71, pp. 1439–1451, 2024, doi: 10.1109/TEM.2022.3158390.
- [22] T. Ahmad and D. Zhang, "Using the internet of things in smart energy systems and networks," *Sustainable Cities and Society*, vol. 68, p. 102783, May 2021, doi: 10.1016/j.scs.2021.102783.
- [23] T. Nasir *et al.*, "Recent challenges and methodologies in smart grid demand side management: state-of-the-art literature review," *Mathematical Problems in Engineering*, vol. 2021, pp. 1–16, Aug. 2021, doi: 10.1155/2021/5821301.
- [24] R. El-Azab, "Smart homes: potentials and challenges," *Clean Energy*, vol. 5, no. 2, pp. 302–315, Jun. 2021, doi: 10.1093/ce/zkab010.
- [25] M. Meliani, A. El Barkany, I. El Abbassi, A. M. Darcherif, and M. Mahmoudi, "Energy management in the smart grid: State-of-the-art and future trends," *International Journal of Engineering Business Management*, vol. 13, Jan. 2021, doi: 10.1177/18479790211032920.

BIOGRAPHIES OF AUTHORS







Vemulapalli Harika     received a Bachelor of Technology in Electrical and Electronics Engineering from Acharya Nagarjuna University. Masters in Engineering from Andhra University with Power Systems and Automation Specilization Pursuing Ph.D. in Electrical Engineering from Andhra University Currently working as an Assistant professor in Electrical and Electronics Engineering Department at Prasad V Potluri Siddartha Institute of Technology, Vijayawada, India. Her research interests include electrical power systems, optimization techniques. She can be contacted at email: vemulapalliharika2312@gmail.com.







Gudavalli Madhavi     received a Bachelor of Technology in Electrical and Electronics Engineering from JNT University, Hyderabad. Master of Technology from Acharya Nagarjuna University with Power Systems Specilization. Pursuing Ph.D. in Electrical Engineering from JNTUK, Kakinada. Currently working as an Assistant professor in Electrical and Electronics Engineering Department at Prasad V Potluri Siddartha Institute of Technology, Vijayawada, India. Her research interests include electrical power systems, optimization techniques. She can be contacted at email: gudavalli.madhavi@gmail.com.







Hanumantha Rao Battu     received M.Sc. And M.Tech. degrees in Computer Science and Engineering, MBA degree in HR and received Ph.D. degree in Computer Science and Engineering. He is currently an associate professor in Computer Science and Engineering Department with the Koneru Lakshmaiah Education Foundation (KLEF), KLEF Deemed to be University, Vaddeswaram, Guntur, India. He worked in various positions in Engineering colleges and P.G. Institutions. His research areas of interest are software engineering, computer networks, and operating systems. He can be contacted at email: hanuma9999@yahoo.com.







Rambabu Kasukurthi     received the B. Tech. degree in Electrical and Electronics Engineering from V.R.S and Y.R.N College of Engineering and Technology, Chirala, India, in 2007 and the M. Tech. degree in Electrical and Electronics Engineering with Power System Engineering Specialization from Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, India in 2011 and pursuing Ph.D. in Andhra University. Currently, he is an Assistant Professor at the Department of Electrical and Electronics Engineering, Aditya University Surampalem, India. His research interests include electrical power systems, faulty analysis, automatic power generation control, and artificial intelligence applied in automatic power generation. He can be contacted at email: rambabu.k@adityauniversity.in and rambabu.kasukurthi@gmail.com.



Pradeep Jangir     is currently associated with the Department of Biosciences, Saveetha School of Engineering. Saveetha Institute of Medical and Technical Sciences, Chennai, India. He is internationally recognized for his advances in swarm intelligence and optimization. He has published over 100 publications with more than 5000 citations and an H-index of 33. His research interests include many-objective, robust optimization, power system engineering optimization, multi-objective optimization, swarm intelligence, evolutionary algorithms, and artificial neural networks. He is working on the application of multi-objective, many-objective, and robust meta-heuristic optimization techniques as well. He can be contacted at email: pkjmttech@gmail.com.



John T Mesia Dhas     received the M.E. degree in Computer Science and Engineering from Sathyabama University, Chennai, India, in 2011. The Ph.D. degree in Computer Science and Engineering from Vel Tech University, Chennai, India, was awarded in 2019. The Post Doctoral Fellowship (PDF) in Computer Science and Engineering from Lincoln University College Malaysia in 2024. Currently, he is an associate professor at the School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India. He is doing research and guiding research scholars in the domains of artificial intelligence, cyber security, and data science. He can be contacted at email: jtmahasres@gmail.com.