

PAANN-ProAct Autoencoder Neural Network Model for Energy Efficient and Robust Anomaly Detection in WSN

¹Geeta and ²Dr. Renuka Arora

¹Research scholar, CSE, Jagannath University, Delhi NCR Haryana

²Professor and Research Supervisor, CSE, Jagannath University, Delhi NCR Haryana

Received: 14th June, 2026; Revised: 20th July 2026; Accepted: 20th August, 2026; Available Online: 15th September 2026

ABSTRACT

Wireless Sensor Networks (WSNs) are extensively employed in environmental monitoring, healthcare, industrial automation, military surveillance, and security applications. However, the limited energy, computational capacity, and communication resources of sensor nodes make efficient anomaly detection a challenging task. Malicious attacks, sensor faults, communication failures, and abnormal measurements can further degrade network reliability and reduce its operational lifetime. To overcome these challenges, this research proposes a ProAct Autoencoder Neural Network (PAANN) for energy-efficient and robust anomaly detection in WSNs. The proposed approach employs a cluster-based architecture in which sensor nodes perform local data processing and anomaly detection, while cluster heads aggregate the relevant information and forward significant anomaly events to the base station. The PAANN model utilizes an autoencoder to learn normal sensor-data patterns and detect abnormal observations based on reconstruction errors. Spatial correlation among neighboring sensor nodes is incorporated to improve anomaly identification and localization. An erroneous-decision abstainer mechanism is also introduced to reduce false-positive alerts and unnecessary computational operations. Furthermore, the Ascendable Energy Coherent Array-based Anomaly Detection (AECAAD) mechanism is incorporated to improve energy efficiency and identify potential Denial-of-Service (DoS) attacks from abnormal communication patterns. Huffman and Arithmetic Coding techniques are employed to compress data before transmission, thereby reducing communication overhead, bandwidth consumption, and energy expenditure. The proposed framework is designed to provide accurate and timely anomaly detection while extending network lifetime and improving the reliability, security, and robustness of WSNs.

Keywords: Wireless Sensor Networks, Anomaly Detection, Deep Learning, Autoencoder; Energy Efficiency; Spatial Correlation; DoS Attack Detection

How to cite this article: Geeta, Renuka Arora, PAANN- ProAct Autoencoder Neural Network Model for Energy Efficient and Robust Anomaly Detection in WSN Int J Drug Deliv Technol. 2026;16(86s): 212-217; DOI: 10.25258/ijddt.16.86s.25

Source of support: Nil.

Conflict of interest: None

1. INTRODUCTION

Among the most often used wireless communication networks are wireless networks of sensors (WSNs), in which nodes for sensors serve as the primary backbone [1,2]. In terms of configuration, WSNs can feature homogenous or heterogeneous sensors, ranging in quantity from hundreds to thousands. The majority of wireless sensor networks (WSNs) are tailored to specific applications, and typically, their sensor nodes have some fundamental functions including monitoring, analysing, calculations, and transmission. Radio frequency electromagnetic pulses are used mostly for communication with nearby nodes [3]. In addition, a base station (BS) functions as a centralized node in the WSN infrastructure, receiving and transmitting monitored data from [4] sensor nodes at a designated area. WSNs are operation-based interactions of communication, meaning that a transmission network is constructed and sensors are placed in the monitoring field in accordance with a specific use case. Wide-open areas are typically where [5] WSNs are

installed for tracking and monitoring purposes [6]. Programs of surveillance include the rubber industry, the pharmaceutical business for hazardous gas monitoring, and patient health surveillance.

Additionally, WSN technology can be utilized for tracking applications including tracking pets, tracking wild species, and [7] tracking humans. Micro-electromechanical systems (MEMS) are among the hardware that have been released recently [8]. Recent advancements in WNS technology have resulted in more inventive frameworks for more affordable and reliable networked communication.

One way to lessen the computing burden of detection methods in nodes is to distribute the anomaly detection process among the nodes in a wireless sensor network (WSN). Nevertheless, the interaction cost resulting from transferring [9] massive volumes of data amongst nodes should also be taken into account when constructing any distributed detection model. A few dispersed detection of

*Author for Correspondence: Geeta

anomaly designs [10], including those found in [11], have been created with communication-related costs in mind. In order to create a global detection model, the distribution concept in these works depends on each node using its resources to implement the anomaly detection method [12] and then transmitting only the highlights of the local detection model to the central location, such as the head of the cluster or base station, for processing. After that, the overall framework is sent back to the routers so they can use it to [13] identify anomalies in further assessments. In WSN, a decentralized divergence recognition approach was presented in [14] to prevent needless estimation and interaction. The kernel density estimator, a non-parametric statistical method, served as the foundation for the creation of this framework. This model did not employ the hierarchical structure [15] that is typically utilized to construct distributed solutions. Rather, the hierarchical framework was imitated by allocating, [16] according to physical closeness, each set of low-capacity detectors to one of a few more capable sensors. In [17], an over-network identification of outliers approach was put forth to lower the transmission congestion that comes with huge data transfer in [18] wireless sensor networks.

The algorithm used to identify the global abnormalities [19] in WSN was based on distance similarity. In this approach, every node searches for anomalies using the distance similarity metric and then broadcasts the results to its neighbours. Until all nodes reach a consensus regarding anomalies [20], other nodes carry out the identical task. Significant energy usage is a result of broadcasting communications. When dealing with large-scale WSNs, the issue worsens.

2. LITERATURE REVIEW

In order to enhance the Quality of Services of IWSN, this research suggests a unique environmentally friendly inter-cluster distribution and failure control approach [21]. The main objective of the proposed system is to implement the Hybrid ANFIS Reptile Optimizing Method, which finds the best path from clustering to sink. Therefore, a fault identification approach based on adjusted supervising may be used to identify a range of IWSN problems, such as residual energy blame, transmission mistakes, and recognizing failure. The evaluation of the suggested structure is calculated with a thousand connections and two distinct sink placements. Subsequently, the research's findings confirm that the suggested model outperforms the current inter-cluster routing techniques, achieving a 0.01 J decrease in energy use.

The recommended study in [22] aims to create an enhanced ecologically conscious route system that can identify abnormalities based on LOF and SVM. The primary goal of the strategy being studied is to develop an algorithm for routing that can identify anomalies in the environment, reduce energy usage, and increase the security and lifetime of the entire network. The effectiveness and competency of the proposed method were evaluated by simulation with the sensing data from the Intel Berkeley Development Lab. Following the

simulation results, an improved energy-efficient routing system with an extra steady neighbourhood as well as an extended network lifetime is developed through the recognition of anomaly networks. When utilizing LOF, the suggested method produces the best outcome.

The incorporated weighed statistics used within the energy-effective weighted-based process (EEWBP) approach in [23] consideration for the node's efficiency, the amount of remaining electrical power, the total number of neighbouring nodes, the conventional flaunting accelerated motions, and the confidence value between the other system elements. These elements are evaluated independently and then merged to aid in cluster creation and node organization. The process of creating multiple collections of SNs, all of which have a head of the cluster (CH), is made simpler by our suggested procedure. This technique allows data to be delivered throughout groups in an environmentally friendly manner, extending the coverage's persistence. The investigation assessed and tested our cluster-based routing strategy using various attributes of the network following it was put into practice.

An Industrial 4.0 node sensor optimization for energy methodology is proposed in this [24] research. The concepts concerning energy gathering, conservation, and efficiency constitute the foundation of the architecture. Its objective is to maximize sensor node energy usage while preserving functioning. The architecture uses dynamic power management, scheduling, and harvesting to reduce fossil fuel consumption lacking sacrificing effectiveness. Furthermore, the structure uses AI and sophisticated analytics to forecast energy use, offering a thorough method of energy optimization. With 96.93% sensibilities, 91.36% incorrect recognition rate, 11.28% erroneous excluding rate, 90.12% prevalent limitation, and 91.24% threatening result, the recommended model performed admirably. It is anticipated that the proposed design will enhance Industry 4.0 sensor node performance, resulting in higher efficiency and lower costs.

This paper [25] proposes a method for Internet of Things node energy anomaly detection based on transmitting information processing. We leverage energy-related through peer-to-IoT transaction analytics and connect excellent information collected from a publicly available dataset. First, our approach looks at and identifies the important aspects of communication of data for Internet of Things emitters using logistic models. The descending distribution is then adjusted using a deep neural network to concentrate on the important elements. By reducing the related reconstructing mistakes, this change improves anomalous recognition precision. Lastly, nodes can use information gathered from resource stabilization to modify the data transfer arrangement for upcoming talks. Simulations demonstrate that the suggested method operates better in abnormal energy recognition than the most advanced unstructured classifiers.

The LEACH algorithm and Sub-cluster LEACH network algorithms are two energy-efficient strategies that will be

examined in the present article [26]. Levenberg-Marquardt neural network (LMNN) as well as Moth-Flame optimization are carried out once after the other to provide improved network efficiency. The level of service is measured by QoS measures like as energy efficiency, the ratio of packet delivery (PDR), efficiency, and delay at the end of the tunnel. Results from simulations subsequent to deployment demonstrate that Sub-cluster LEACH using MFO executes better than alternative algorithms. In addition, identifying anomalies employing artificial intelligence techniques like KNN, SVM, and LR was covered in the second half of the article. A new anomaly recognition approach is then suggested after taking into account the NSLKDD database. According to simulation findings, the suggested strategy using SVM yields superior outcomes than both of the other methods.

3. PROBLEM STATEMENT

Industries such as military service observation, healthcare monitoring as well as ecological of the environment depend on WSNs, or wireless sensor networks, for transmitting information and collecting. Numerous nodes with sensors make up these computer networks, which collect information and then send it to the center for evaluation. In WSNs, collected data is necessary to minimize redundancies as well as optimize communication latency. Nevertheless, anomalous data may negatively impact the reliability and validity of the aggregated data. As a result, anomaly detection (AD) is essential for locating inaccurate information as well as guaranteeing the accuracy and consistency of knowledge. The brief lifespan of devices containing sensors and insufficient sources of energy are two of WSNs' primary drawbacks. The confidentiality of information must be preserved whilst consumption of energy is minimized in anomaly systems for detection. Excessive consumption of energy can cause premature node sensor mortality, which shortens the network's service life as well as overall efficacy. WSNs are potentially susceptible to a range of privacy-related concerns, including DoS assaults, because of inherent transparent architecture. By depleting the sensing systems' assets attacks like these could prevent the network from operating normally. Node sensors have minimal electrical capacity, which makes it impossible to implement sophisticated techniques for network authorization, rendering traditional protection considerations unworkable. Numerous causes, such as malevolent assaults, insufficient planning, and equipment issues, can lead to anomalous incidents in WSNs. Preserving the credibility and general efficacy of the entire system depends on the early detection of these kinds of abnormalities. Combining cloud-based algorithms for recognizing anomalies elevated connectivity costs and significant use of energy at sensor node locations made them unfeasible for enterprises requiring instantaneous supply, along with other disadvantages. The present study has investigated the usage of distributed anomalous identification techniques based on Deep Neural Networks (DNNs) to overcome the drawbacks of centrally managed systems. These scattered approaches provide real-time

recognition of anomalies despite greatly reducing sensor-to-cloud transmission by deploying replicas of the anomaly recognition architecture at the positions of the detecting nodes. Protecting the privacy of information and dependability in WSNs requires the capacity to recognize abnormalities. The problems produced by centralized management procedures may be resolved by the distributed DNN-based strategy, especially in terms of energy conservation, decreased delay, and more affordable communication charges. The objective of this study is to improve these approaches in order to guarantee accurate and timely detection of anomalies in WSNs, consequently augmenting their general robustness as well as effectiveness.

4. PROPOSED METHODOLOGY:

The recommended techniques for improving the detection of anomalies in Wireless Sensor Networks (WSNs) are through the implementation of mathematical systems of neural networks and sophisticated coding techniques. The main goals are to decrease the number of false positives, utilize fewer resources, and increase the accuracy of recognizing anomalies. As such, wireless sensor networks (WSNs) employ the **ProAct Autoencoder neural network model (PAANN)** to accurately and efficiently identify anomalous conditions. Automatic encoders are skilled at spotting variations that point to anomalous since systems are accustomed to the typical patterns of information. The network is first divided into clusters, each of which is supervised by a cluster head who is in control of local data aggregation and anomaly detection. The collected data has undergone processing to eliminate extraneous knowledge and distortion. The encoder compresses the input information into a space of latent information democracy, and a decoding program reassembles the input information from this model to form the auto-encoder. In order to identify anomalies based on spatial patterns, sensor nodes within a cluster correlate their spatial data. By recognizing the identical and distinct network identities implicated in the assault, spatial correlational analysis aids in localizing attackers inside the system. An encoder compresses the input information into a space of latent information democracy, and a decoder recreates the input information from this model to form the auto-encoder. Standard instances of information are used to train the network in order to reduce reconstruction errors between the input and the output. In order to reduce false positives and guarantee that only fundamental abnormalities cause warnings, the model includes features that prevent needless data loss through a novel **erroneous-decisive abstainer mechanism**. In addition to minimizing the computational demands on individual sensor nodes and saving energy, cluster-level anomalies are transmitted to the base station for additional investigation. The network's lifespan can be increased using the Ascendable Energy Coherent Array-based Anomaly Detection (AECAAD) method, which efficiently identifies DoS assaults, eliminating the need for essential management techniques. Data transmission and anomaly detection require less energy when aggregation is employed. Identifying

possible DoS attacks is aided by tracking data transmission patterns inside clusters. Anomalies that are discovered produce notifications sent to the base station, thus reducing pointless communication. In order to reduce the amount of data sent from sensors to clouds while retraining distributed anomaly detection models, **two-fold intact compilation algorithms, Arithmetic Coding, and Huffman Coding** are examined and employed in execution. This reduces the overall amount of the data by compressing the data by allocating more extended codes to less frequent values for information and shorter codes to

more frequent information variables. In accumulation, it reaches better compression ratios for specific data types by representing a series of symbols as a single number in the interval $[0, 1]$. Before sending updated samples of standard data to the cloud in order to retrain the algorithms, the nodes with sensors encrypt them. Sensor node resources are conserved when data is encoded and transmitted with reduced bandwidth and energy. When the compressed data is received, the cloud node decodes it and returns it to its natural format so the models can be trained again.

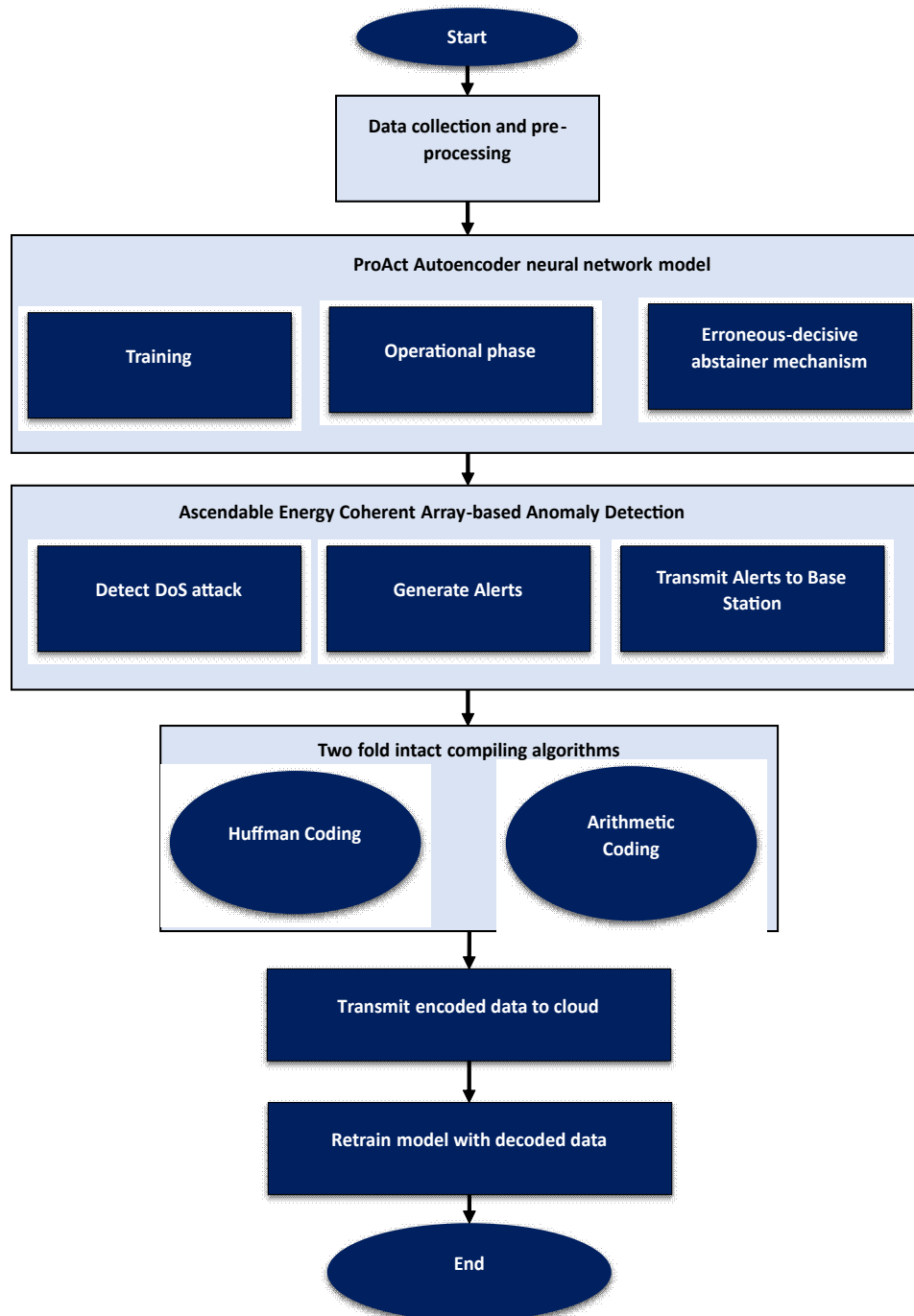


Figure: Proposed block diagram

5. EXPECTED OUTCOME

The research seeks to achieve several important goals that will greatly improve Wireless Sensor Networks' (WSNs') performance and dependability through sophisticated anomaly detection techniques. The study predicts a considerable enhancement in anomaly detection precision. The suggested approaches are anticipated to reduce energy usage by streamlining anomaly detection algorithms and cutting down on pointless data transfers. As a result, the sensor nodes and the network's overall operating lifespan will be increased. By identifying abnormalities that suggest possible security breaches, the network can immediately safeguard its integrity and performance, decreasing latency and guaranteeing prompt reactions to potential problems using distributed anomaly detection models at the sensor nodes. In the long term, this will increase the dependability and affordability of WSNs, increasing their worth for numerous complicated applications.

REFERENCES

1. Ketshabetswe, L.K., Zungeru, A.M., Lebekwe, C.K. and Mtengi, B., 2024. A Compression-Based Routing Strategy for Energy Saving in Wireless Sensor Networks. *Results in Engineering*, p.102616.
2. Wang, Z., Wei, Z., Gao, C., Chen, Y. and Wang, F., 2023. A framework for data anomaly detection based on iterative optimization in IoT systems. *Computing*, 105(11), pp.2337-2362.
3. Abdelhamid, A., Elsayed, M.S., Jurcut, A.D. and Azer, M.A., 2023. A lightweight anomaly detection system for black hole attack. *Electronics*, 12(6), p.1294.
4. Tabbassum, S. and Pathak, R.K., 2024. Effective data transmission through energy-efficient clustering and Fuzzy-Based IDS routing approach in WSNs. *Virtual Reality & Intelligent Hardware*, 6(1), pp.1-16.
5. Krishnamoorthy, V.K., Izonin, I., Subramanian, S., Shandilya, S.K., Velayutham, S., Munichamy, T.R. and Havryliuk, M., 2023. Energy saving optimization technique-based routing protocol in Mobile ad-hoc network with IOT Environment. *Energies*, 16(3), p.1385.
6. Srivastava, J. and Prakash, J., 2023. Multi-modal for Energy Optimization and Intrusion Detection in Wireless Sensor Networks. *Wireless Personal Communications*, 133(1), pp.289-321.
7. Sheeja, S., 2024. SHAKE-ESDRL-based energy efficient intrusion detection and hashing system. *Annals of Telecommunications*, 79(5), pp.381-396.
8. Hu, L., Han, C., Wang, X., Zhu, H. and Ouyang, J., 2024. Security Enhancement for Deep Reinforcement Learning-Based Strategy in Energy-Efficient Wireless Sensor Networks. *Sensors*, 24(6), p.1993.
9. Lakshmi, M.S., Ramana, K.S., Ramu, G., Shyam Sunder Reddy, K., Sasikala, C. and Ramesh, G., 2024. Computational intelligence techniques for energy efficient routing protocols in wireless sensor networks: A critique. *Transactions on Emerging Telecommunications Technologies*, 35(1), p.e4888.
10. Surenter, I., Sridhar, K.P. and Roberts, M.K., 2023. Maximizing energy efficiency in wireless sensor networks for data transmission: A Deep Learning-Based Grouping Model approach. *Alexandria Engineering Journal*, 83, pp.53-65.
11. Saleh, H.M., Marouane, H. and Fakhfakh, A., 2024. Stochastic gradient descent intrusions detection for wireless sensor network attack detection system using machine learning. *IEEE Access*.
12. CL, A. and Sumathi, R., 2023. Anomaly detection in WSN IoT (Internet of Things) environment through a consensus-based anomaly detection approach. *Multimedia Tools and Applications*, pp.1-20.
13. El-Sayed, W.M., El-Bakry, H.M. and El-Sayed, S.M., 2023. Integrated data reduction model in wireless sensor networks. *Applied Computing and Informatics*, 19(1/2), pp.41-63.
14. Khan, S.U., Khan, Z.U., Alkhowaiter, M., Khan, J. and Ullah, S., 2024. Energy-efficient routing protocols for UWSNs: A comprehensive review of taxonomy, challenges, opportunities, future research directions, and machine learning perspectives. *Journal of King Saud University-Computer and Information Sciences*, p.102128.
15. Subalakshmi, N., 2024. INTELLIGENT SCHEDULING OPTIMIZATION FOR ENERGY-EFFICIENT MULTICAST ROUTING IN CLOUD BASED WIRELESS NETWORKS. *Technology and Society*, p.262.
16. Rajasoundaran, S., Kumar, S.S., Selvi, M., Thangaramya, K. and Arputharaj, K., 2024. Secure and optimized intrusion detection scheme using LSTM-MAC principles for underwater wireless sensor networks. *Wireless Networks*, 30(1), pp.209-231.
17. Al-Atawi, A.A., 2023. Extending the Energy Efficiency of Nodes in an Internet of Things (IoT) System via Robust Clustering Techniques. *International Journal of Computer Networks and Applications*.
18. Prasad, K.V. and Periyasamy, S., 2023. Secure-Energy Efficient Bio-Inspired Clustering and Deep Learning based Routing using Blockchain for Edge Assisted WSN Environment. *IEEE Access*.
19. Ramamoorthi, S. and Appathurai, A., 2023. Energy aware Clustered blockchain data for IoT: An end-to-end lightweight secure & Enroute filtering

- approach. *Computer communications*, 202, pp.166-182.
20. Hota, L., Nayak, B.P. and Kumar, A., 2024. Algorithms for Optimization and in Intelligence Wireless Networks. *5G and Beyond Wireless Communications: Fundamentals, Applications, and Challenges*, p.306.
21. Vazhuthi, P.P.I., Prasanth, A., Manikandan, S.P. and Sowndarya, K.D., 2023. A hybrid ANFIS reptile optimization algorithm for energy-efficient inter-cluster routing in internet of things-enabled wireless sensor networks. *Peer-to-Peer networking and applications*, 16(2), pp.1049-1068.
22. Sharma, T., Mohapatra, A.K. and Tomar, G., 2023. A novel SVM and LOF-based outlier detection routing algorithm for improving the stability period and overall network lifetime of WSN. *International Journal of Nanotechnology*, 20(5-10), pp.759-789.
23. Kaur, P., Kaur, K., Singh, K. and Kim, S., 2023. Early forest fire detection using a protocol for energy-efficient clustering with weighted-based optimization in wireless sensor networks. *Applied Sciences*, 13(5), p.3048.
24. Sivakumar, S., Logeshwaran, J., Kannadasan, R., Faheem, M. and Ravikumar, D., 2024. A novel energy optimization framework to enhance the performance of sensor nodes in Industry 4.0. *Energy Science & Engineering*, 12(3), pp.835-859.
25. Bushehri, A.S., Amirnia, A., Belkhiri, A., Keivanpour, S., De Magalhaes, F.G. and Nicolescu, G., 2023. Deep Learning-Driven Anomaly Detection for Green IoT Edge Networks. *IEEE Transactions on Green Communications and Networking*.
26. Masood, F., Khan, M.A., Alshehri, M.S., Ghaban, W., Saeed, F., Albarakati, H.M. and Alkhayyat, A., 2024. AI-Based Wireless Sensor IoT Networks for Energy-Efficient Consumer Electronics Using Stochastic Optimization. *IEEE Transactions on Consumer Electronics*.