Journal of Industrial Intelligence
https://www.acadlore.com/journals/JII

Machine Learning-Driven IDPS in IIoT Smart Metering Networks

Qutaiba I. Ali[1*] Sahar L. Qaddoori[2]

[1]Computer Engineering Department, Engineering College, University of Mosul, 41003 Mosul, Iraq
[2]Electronic Engineering Department, Electronics Engineering College, Ninevah University, 41003 Mosul, Iraq

* Correspondence: Qutaiba I. Ali (qut1974@gmail.com)

Received: 02-10-2025 **Revised:** 03-13-2025 **Accepted:** 03-24-2025

Citation: Q. I. Ali and S. L. Qaddoori, "Machine learning-driven IDPS in IIoT smart metering networks," *J. Ind Intell.*, vol. 3, no. 1, pp. 30–43, 2025. https://doi.org/10.56578/jii030104.

Abstract: The proliferation of the Industrial Internet of Things (IIoT) has transformed energy distribution infrastructures through the deployment of smart metering networks, enhancing operational efficiency while concurrently expanding the attack surface for sophisticated cyber threats. In response, a wide range of Machine Learning (ML)–based Intrusion Detection and Prevention Systems (IDPS) have been proposed to safeguard these networks. In this study, a systematic review and comparative analysis were conducted across seven representative implementations targeting the Internet of Things (IoT), IIoT, fog computing, and smart metering contexts. Detection accuracies reported in these studies range from 90.00% to 99.95%, with models spanning clustering algorithms, Support Vector Machine (SVM), and Deep Neural Network (DNN) architectures. It was observed that hybrid Deep Learning (DL) models, particularly those combining the Convolutional Neural Network and the Long Short-Term Memory (CNN-LSTM), achieved the highest detection accuracy (99.95%), whereas unsupervised approaches such as K-means clustering yielded comparatively lower performance (93.33%). Datasets utilized included NSL-KDD, CICIDS2017, and proprietary smart metering traces. Despite notable classification accuracy, critical evaluation metrics—such as False Positive Rate (FPR), inference latency, and computational resource consumption—were frequently underreported or omitted, thereby impeding real-world applicability, especially in edge computing environments with limited resources. To address this deficiency, a unified benchmarking framework was proposed, incorporating precision-recall analysis, latency profiling, and memory usage evaluation. Furthermore, strategic directions for future research were outlined, including the integration of federated learning to preserve data privacy and the development of lightweight hybrid models tailored for edge deployment. This review provides a data-driven foundation for the design of scalable, resource-efficient, and privacy-preserving IDPS solutions within next-generation IIoT smart metering systems.

Keywords: Industrial Internet of Things; Smart metering; Intrusion detection and prevention; Anomaly detection; Machine learning; Edge computing; Federated learning; Benchmarking framework

1 Introduction

Everything globally, from body sensors to contemporary cloud computing, is included in IoT. It creates a sophisticated distributed system by connecting humans, machines, and networks everywhere. In addition, it improves the quality of human life by enabling reliable Machine-to-Machine (M2M) and Machine-to-Human (M2H) connections [1]. The integration of conventional IoT principles in manufacturing industries and applications is referred to as IIoT [2]. In the recent decade, IIoT has emerged as the most rapidly evolving revolutionary technology, with the ability to digitize and connect numerous industries, resulting in significant economic prospects and global Gross Domestic Product (GDP) growth [3, 4]. Smart metering, factories, grids, cities, homes, linked autos, and supply chain management are just a few of the IIoT's applications [2].

The vast number of sensors in the IIoT network generates a tremendous volume of data [3]. The edge devices collect data from appliances and send it to local servers after performing any essential preprocessing. Then, local servers are utilized to connect edge devices and cloud servers [2].

With the broad deployment of smart meters, it is now possible to add the smart meter's function to the edge device. The smart meter is one of the main components of the smart metering network, which is used to learn regular power operating usage and detect or flag abnormal usage. User behavior, human mistakes, and underperforming equipment contribute to wasted energy in buildings and industries. Identifying anomalous consumption power behavior can

help reduce peak energy usage and change undesirable user behavior. The average power consumption characteristic distribution of the smart meter data is relatively regular and has noticeable periodicity, but aberrant power consumption lacks these features. Therefore, it can be assumed that often-observed daily patterns represent usual consumption behaviors during the day, while rarely-observed patterns represent unusual consumption behaviors [5].

Monitoring and regulating such infrastructures simultaneously is important to provide an adequate degree of security for the IIoT networks. Intrusion Detection System and Intrusion Prevention System (IDS/IPS) are the most often used systems for achieving this goal [6]. The former monitors intrusions and occurrences of safety violations and notifies people when they happen. On the other hand, the latter takes further steps to avoid an attack, mitigate its consequences, or respond actively to a security breach [7, 8].

Signature- and anomaly-based detection are the two common detection methods used by IDS. By evaluating network data for specified patterns, signature-based detection approaches are successful in detecting well-known threats. Attacks are detected via anomaly-based detection systems, which monitor the behavior of the entire system, traffic, or objects and compare it to a preset normal state [9–11]. Anomaly-based IDS provides greater generic properties than signature-based IDS because of ML approaches [10, 12].

An important direction is the use of ML algorithms for anomaly-based IDS approaches. The general aspects of the training traffic information are learned by ML techniques. The input traffic information can be accurately detected based on the learned attributes. Conventional ML methods, on the other hand, do not demand a lot of processing power from the hardware and have a short training time, making them more suited to the needs of IIoT edge devices [13, 14].

IIoT, particularly in smart metering, enhances operational efficiency but significantly increases cybersecurity risks due to expanded connectivity. Despite many ML-based IDPS being proposed, current research suffers from three key limitations: reliance on outdated datasets and a lack of multi-metric evaluation (e.g., latency and false positives) and comparative analysis. This review addresses these gaps by presenting a performance-driven statistical comparison of existing IDPS methods. It highlights trade-offs between accuracy and efficiency, reveals the strengths of DL models, and proposes a unified benchmarking framework to guide future development of scalable and practical security solutions for IIoT smart metering networks.

The objectives of this study are:

• To analyze security threats and vulnerabilities in IIoT-based smart metering networks.

• To review existing intrusion detection methodologies and their applicability in IIoT environments.

• To evaluate the effectiveness of the proposed system through performance metrics such as detection accuracy, computational efficiency, and response time.

2 IoT Application Domain

The development of IoT applications is an ongoing process, but several significant challenges must be addressed. These include issues related to security, privacy, complexity, scalability, and ensuring adequate spectrum availability to connect a vast number of devices and sensors [15]. IoT systems must be capable of processing data in real time and establishing seamless connectivity among various devices. In addition to handling sensing and actuation tasks, IoT applications are expected to support interactions involving humans, such as Human-to-Machine (H2M), Human-to-Human (H2H), and M2M communication [16].

IoT is not restricted to enhancing individual aspects of daily life like smart homes or intelligent buildings. Its applications extend across numerous sectors, including agriculture, healthcare, smart business solutions, finance, and environmental monitoring [16]. These applications can be differentiated based on several criteria such as network availability, coverage area, scalability, frequency of use, diversity, and user engagement.

Based on these criteria, IoT applications are typically grouped into four main categories: personal and home, enterprise, utility, and mobile. As illustrated in Figure 1, personal and home IoT applications operate at an individual or household level, while enterprise applications target communities. Utility-based IoT applications are designed for large-scale implementations at regional or national levels. Mobile IoT, due to its wide-ranging connectivity, often overlaps with the other categories [17, 18].

IoT functionalities are often divided based on usage areas into four main domains: monitoring (e.g., tracking environmental conditions and device status and sending alerts), control (managing device operations), optimization (e.g., diagnostics, repair, and performance enhancement), and autonomy (enabling devices to operate independently) [19, 20].

Table 1 outlines the primary IoT application areas currently emphasized in academic and industry research, along with representative examples for each category [21, 22]. Each domain contains a range of existing use cases, with many more under development and expected to be implemented in the near future [17].

The smart metering network is a key component of modern power communication systems, integrating electrical and telecommunications infrastructure to enable the collection, monitoring, and analysis of electricity consumption data. This system typically includes smart meters, data concentrators, and a head-end system, and is structured across multiple layers of communication network [23, 24].

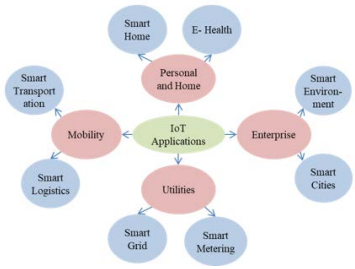

Figure 1. IoT application domains and their examples

Table 1. Main IoT application domains

Application Domains	Examples of Application
Home automation	Remote control applications, building automation, water use, and energy use
Retail & logistics	Stock control, smart shopping, e-payments, supply chain control, fleet tracking, item tracking, and smart product management
E-health	Patient monitoring, patient surveillance, personnel tracking, doctor tracking, predictive expertise information to assist doctors and practitioners, and real-time patient-health status monitoring [23–26]
Smart animal farming	Meat traceability and animal monitoring
Security and emergency	Perimeter control and tracking, and disaster recovery
Smart cities	Structural health, traffic congestion, participatory sensing, smart traffic lights, smart parking management, and accident detection
Smart transportation	Smart transportation through real-time dynamic on-demand traffic information and shortest-time travel path optimization
Smart metering	Metering of heating systems, and metering in the smart electric grid
Industrial control	Mobile robotics applications in industry, and manufacturing applications
Smart environment	Forest fire detection, remote seismography, pollution monitoring, air pollution, and noise monitoring
Smart water	Level monitoring, flood detection, and water leakage detection
Smart agriculture	Moisture management, crop monitoring, compost, soil, irrigation management, and smart greenhouses

The network is generally divided into three main segments: the Home Area Network (HAN), which connects smart meters with household appliances; the Neighborhood Area Network (NAN), which links multiple smart meters to a data concentrator; and the Wide Area Network (WAN), which connects multiple NANs to the utility's central management system or head-end [25]. Communication within the smart metering network can occur over both wired and wireless mediums and supports two-way data exchange between components.

Each network tier operates under different constraints. WAN supports high-speed, long-distance communication and often transmits sensitive data, necessitating secure and reliable infrastructure. In contrast, NAN and HAN function over shorter distances and at lower communication speeds. HAN, in particular, is constrained by limited computing and storage resources and is more vulnerable to cybersecurity threats such as Denial-of-Service (DoS) attacks, especially due to the connectivity of smart appliances to the internet [26, 27].

An overview of the smart metering network's architecture is illustrated in Figure 2.

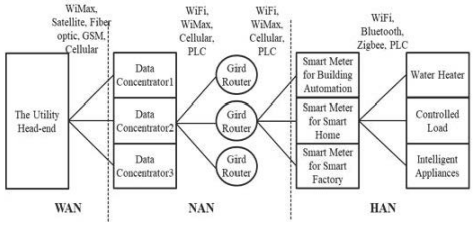

Figure 2. Communication structure of the smart metering network

3 Methodology

This review follows a structured approach to identify, select, and evaluate ML-based IDPS applied to IIoT smart metering environments. To ensure relevance and quality, peer-reviewed studies published between 2016 and 2023 that met the following criteria were included in this study:

- The study proposes or evaluates an IDPS that incorporates ML techniques.
- The solution targets either IIoT, smart grid, or smart metering networks.
- The study reports at least one quantitative performance metric (e.g., accuracy, detection rate, and FPR).
- The study uses publicly available or described datasets for evaluation.

Studies focused purely on cryptographic security, protocol design, or high-level architectural proposals without ML-based detection mechanisms were excluded. The selected studies were classified into three domains: general IoT/IIoT networks, smart metering with power anomaly detection, and combined IDS for IIoT smart metering.

Within each domain, models were categorized by algorithm type (e.g., SVM, DNN, CNN-LSTM, K-means) and whether they were supervised, unsupervised, or hybrid approaches. Preference was given to studies that presented results using real-world or widely accepted datasets (e.g., NSL-KDD, CICIDS2017, and Pecan Street).

To analyze model effectiveness, the following performance indicators were extracted when available:

- Detection accuracy (%)
- FPR
- Latency (ms)
- Deployment level (edge, gateway, or centralized)

Then a comparative matrix was created to evaluate trade-offs across model types and deployment domains. In cases where only detection accuracy was reported, the lack of a full-spectrum evaluation was noted as a limitation. Bar charts and summary tables were generated to visualize trends and highlight model strengths and weaknesses. This study focused on commonly adopted and impactful models such as SVM, Random Forest (RF), DNN, and CNN-LSTM due to their frequent appearance in IIoT security literature and diverse performance characteristics. Lightweight models like K-means and Isolation Forest (iForest) were also included to explore their suitability for edge-constrained environments.

A critical factor in evaluating the effectiveness of ML-based IDPS solutions is the dataset used for training and testing. Table 2 summarizes the datasets employed in the studies reviewed, highlighting their origin, content type, and suitability for IIoT smart metering contexts. These datasets were selected by the original studies primarily due to availability, annotation completeness, and community acceptance. However, several limitations are evident:

- A lack of domain specificity: Many studies have used general-purpose IDS datasets (e.g., NSL-KDD), which do not capture the unique communication patterns and vulnerabilities of the smart metering networks.
- Insufficient diversity: Most datasets focus on specific traffic types or limited device behaviors, reducing the generalizability of trained models.
- Limited public access: Several promising datasets (e.g., SGCC) are not publicly available, hindering reproducibility and cross-study benchmarking.

Table 2. Datasets employed in this study

Dataset	Source/Provider	Type	Typical Use Domain	Notes on Relevance
NSL-KDD	Canadian Institute for Cybersecurity	Network traffic data	General IDS (IoT/IIoT)	Popular but outdated; lacks modern IIoT-specific patterns
CICIDS2017	Canadian Institute for Cybersecurity	Realistic traffic (multi-attack)	IIoT and smart grid	Rich and modern; includes multiple attack types
Pecan Street	Real-world smart meter data	Electricity consumption	Smart metering	Appliance-level data, suitable for anomaly detection
KDD Cup '99	UCI Repository	Network intrusion data	Legacy IDS benchmarks	Overused and unrealistic in modern networks
DS2OS	Simulation-based	IIoT service interaction data	IIoT resource allocation	Lightweight, but lacks diversity in traffic
SGCC	Utility provider (China)	Smart grid consumption data	Smart metering	Relevant, but not publicly available
SCT	Simulation with NS3	Smart meter traffic	HAN/NAN simulation	Mimics real-world meter-to-grid interactions

Various studies have yielded many approaches for the IDS in the security of IoT/IIoT networks. Therefore, this study focuses on three domains (IoT, IIoT, and smart metering). The relationship between these domains is shown in Figure 3. As a result, this section is divided into three parts based on Figure 4 that shows the numbers of subsections.

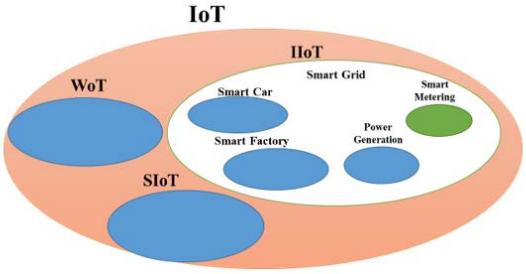

Figure 3. Relationship between IoT, IIoT, and smart metering

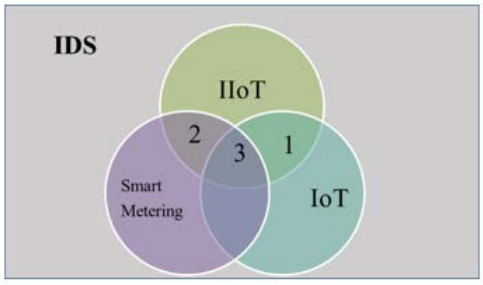

Figure 4. Multiple IDS approaches for the literature review

3.1 IDS-Based IoT/IIoT Networks

In recent years, several researchers have proved that ML models were used to construct the IDS to safeguard IoT/IIoT networks [28, 29]. This subsection presents a brief survey of the literature.

Aydogan et al. [30] proposed a genetic programming-based intrusion detection methodology for IIoT systems, as well as a proof of concept and quantitative assessment. Furthermore, because the network involves a variety of devices with varying capabilities and resource limits, the appropriateness of a central IDS at the root node was investigated. It was demonstrated that the root node could efficiently identify Routing Protocol for Low-Power and Lossy Networks (RPL) attacks in a timely way. Shalaginov et al. [31] developed a new method that allows for the benefits of ML techniques for IoT security while balancing the performance of the model and computational complexity. The use of the Message Queue Telemetry Transport (MQTT) was proposed as the basis for a protocol for updating neural network models on resource-constrained devices. This allows all unessential and demanding model learning and meta-heuristic improvement operations to be moved to more capable IoT gateway devices. Simultaneously, the IoT node devices undergo the less computationally intensive testing phase.

Latif et al. [32] proposed a unique IIoT attack prediction system based on a lightweight random neural network. Using the DS2OS dataset, the suggested system identifies IIoT threats with high accuracy and reduced forecast time. The suggested algorithm's performance was assessed by generating several performance parameters with varied limitations. Maharani et al. [33] suggested identifying attacks in a fog computing environment using numerous ML methods to efficiently detect harmful activity. The evaluation was carried out using the KDD Cup '99 dataset, with K-means, RF, and Decision Tree (DT) algorithms being compared. According to the study by Eskandari et al. [34], Passban is an intelligent IDS that can secure IoT devices that are directly linked to it. The suggested method is unique in that it may be installed directly on low-cost IoT gateways (e.g., single-board personal computers). Passban can identify a variety of malicious activities, such as Secure Shell (SSH) and Hypertext Transfer Protocol (HTTP) brute force, Transmission Control Protocol (TCP) synchronous (SYN) flood, and port scanning assaults, with a low FPR and a high accuracy.

Awotunde et al. [35] developed a DL-based attack detection framework for IIoT networks. A combination of rule-based feature engineering and a deep feed-forward neural network model was used to implement the training procedure. NSL-KDD and UNSW-NB15 datasets were used to evaluate the suggested approach. Raja et al. [36] introduced a two-stage DL-based IDS for IIoT networks. DNNs were trained and evaluated in the first stage of detection. Second-stage detection was fed assaults with a reduced detection rate or precision in the first-stage detection.

DNN and the negative selection algorithm were trained utilizing the dragonfly algorithm and were employed for the second-stage detection. The outputs of both algorithms were combined using Dempster Shafer's combination rule. Their findings compared with datasets from CICIDS 2017, CICIDS 2018, and TON IoT.

Nguyen et al. [37] presented Realguard IDS, a DNN-based network IDS directly run on local gateways to safeguard IoT devices within the network. With a small processing footprint, their concept can accurately identify several cyberattacks in real time. This is accomplished using a simple feature extraction approach and a DNN-based assault detection model. Realguard could identify ten types of attacks, such as port scan, Robot Network (Botnet), and File Transfer Protocol (FTP) Patator, in real time and operate on resource-constrained gateways (Raspberry Pi), according to their analyses on the CICIDS2017 dataset.

Based on Table 2, numerous researchers have presented effective intrusion detection strategies for IoT/IIoT platforms. Nevertheless, the existing research has certain limitations. First, most researchers in recent studies evaluated their schemes by achieving a few performance metrics that do not offer in-depth evaluations. Second, the presented techniques' feasibility for resource-limited devices has not been thoroughly deliberated. Finally, several studies' great experimental accuracy is due to a mixture of feature engineering techniques, such as feature mapping and reduction, with classification algorithms. On the other hand, feature engineering is a time-consuming process that is not suitable for time-critical edge layer devices that have imperfect computational capabilities.

3.2 IDS for IIoT Networks with Smart Metering

In recent years, there has been a notable increase in the use of ML and data mining techniques for analyzing and modeling residential electricity consumption data [38]. As a result, several significant studies have emerged in this field.

Table 3. Details for the recent research based on IDS for IoT/IIoT networks

Ref.	Year	Dataset Used	Algorithm Utilized	Updating Policy	Architectural Approach	Performance Parameters	Prevention and Response Activities	Validation Strategy	Performance Metrics
[30]	2019	N/A	Genetic programming	No	Centralized	Detection efficiency	No	No	Acc=99.83%
[31]	2019	NSL-KDD	Neural network	Yes	Distributed	N/A	No	Yes	N/A
[32]	2020	DS2OS	Random neural network	No	Centralized	Detection efficiency and resource usage	No	Yes	Acc=99.20%
[33]	2020	KDD Cup'99	K-means	No	Centralized	Detection efficiency	No	No	Acc=93.33%
[34]	2020	Generated by author	iForest and local outlier factor	Yes	Distributed	Detection efficiency and resource usage	No	Yes	N/A
[35]	2021	NSL-KDD and UNSW-NB 15	DNN	No	Centralized	Detection efficiency	No	No	Acc1=99% Acc2=98.9%
[36]	2021	CICIDS 2017, CICIDS 2018, and TON IoT	DNN	No	Centralized	Detection efficiency	No	No	Acc1=99.86% Acc2=97.58% Acc3=98.8%
[37]	2022	CICIDS2017	DNN	Yes	Distributed	Detection efficiency and resource usage	Yes	Yes	Acc=99.64%

Note: N/A means not available.

Jokar et al. [39] introduced a Consumption Pattern-Based Energy Theft Detection (CPBETD) system. This method leveraged the predictable behavior of typical consumers and incorporated a known malicious usage pattern to identify irregularities. The system utilized an SVM model to predict target values based on test data. The research,

which used data from the Irish Smart Energy Trial, demonstrated that the CPBETD system achieved both a high accuracy and a strong detection rate.

Similarly, Bhattacharjee et al. [40] investigated four distinct types of data manipulation threats: conflict, camouflage, deductive, and additive. Using the Pecan Street dataset, statistical analysis techniques were applied to detect these falsification attempts. The study yielded promising results, showing a high detection rate with minimal false positive cases. Table 3 shows the details for the recent research based on IDS for IoT/IIoT networks.

García et al. [41] explored the performance of both supervised and unsupervised neural network models for detecting unusual electricity consumption behaviors. The results showed that supervised learning methods notably improved the accuracy of anomaly detection. Similarly, Xiang et al. [42] addressed the challenge of identifying consumption anomalies in large-scale, real-time data streams. They proposed a detection framework built on the Apache Spark in-memory distributed computing system and its Spark Streaming extension. The approach combined supervised learning with statistical techniques and was deployed using a lambda architecture.

Chahla et al. [43] developed an anomaly detection framework to enhance energy efficiency and identify irregular usage behaviors. The method involved training various usage scenarios using the K-means clustering algorithm to represent individual consumption patterns. To forecast energy usage for the upcoming hour, the LSTM model was applied. The approach was evaluated using real energy consumption data from the Pecan Street project in the United States. Himeur et al. [44] introduced a novel method that relies on a rule-based system to extract micro-moment features from user activity patterns, which reflect daily behavior related to energy use. These extracted features were then used in a DL model to improve the detection and classification of abnormal consumption events.

In a study by Oprea et al. [45], two unsupervised techniques were proposed for anomaly detection in unlabeled time-series data: the Spectral Residual (SR)-CNN and a martingale-based model designed to identify shifts in data streams. Additionally, Fisher Linear Discriminant Analysis (LDA) and a two-class boosted DT were applied to refine results on the processed datasets.

Zhang et al. [46] combined the Transformer DL model with K-means clustering to predict future electricity consumption and detect outliers. The Transformer was used to forecast short-term usage, while K-means clustering helped enhance the accuracy of these predictions. Deviations between forecasted and actual consumption were used to flag anomalies.

Table 4. Details for the recent research based on IDS for IoT/IIoT networks

Ref.	Year	Dataset Used	Algorithm Utilized	Updating Policy	Network Field	Place On	Anomaly Type	Validation Strategy	Performance Metrics
[39]	2016	Irish Smart Energy Trial	Multiclass SVM	No	NAN	Data aggregator	Malicious consumption patterns	No	DR=94%
[40]	2017	Pecan Street	Statistical technique	No	N/A	N/A	Data falsification	No	N/A
[41]	2018	UC Irvine	Neural network	No	N/A	N/A	Unexpected electricity consumption	No	N/A
[42]	2019	EERE	Clustering technique	No	NAN	Data aggregator	Abnormal electricity consumption	No	Acc=99.6%
[43]	2019	Pecan Street	K-means and LSTM	No	NAN	N/A	Aberrant activities	No	N/A
[44]	2020	QUD, DRED, and PCSiD	DL	No	NAN	Data aggregator	Energy consumption anomalies	No	Acc=99.58%
[45]	2021	CER and ISSDA	SR-CNN	No	NAN	N/A	Energy consumption anomalies	No	Acc=90%
[46]	2021	UC Irvine	K-means and DL	No	NAN	N/A	Energy consumption anomalies	No	Acc=97%

Note: QUD indicates the Qatar University dataset, EERE indicates the Office of Energy Efficiency and Renewable Energy, UCI indicates the UC Irvine ML repository, and CER and ISSDA indicate the Commission of Energy Regulation and Irish Social Science Data Archive.

As summarized in Table 4, aggregated-level data has limitations in accurately identifying the source of energy consumption irregularities. Consequently, analyzing appliance-level data collected by smart meters is considered more effective for detecting specific anomalies. Additionally, the lack of publicly available platforms for generating realistic energy datasets remains a major obstacle in advancing anomaly detection research in this field.

3.3 IDS in IoT/IIoT networks for smart metering

In recent years, growing attention has been given to the security challenges within IoT and IIoT networks, particularly in the context of smart metering applications. Consequently, numerous intrusion detection strategies have been proposed and developed to address various cyber threats targeting these networks [47].

Sedjelmaci et al. [48] introduced an intrusion detection method tailored for NANs in smart grids. The system, which operates across control centers, smart meters, and data collectors, combines rule-based mechanisms with ML classifiers trained on the KDD 99 dataset. The results demonstrated strong security performance while maintaining low energy consumption. Similarly, Jindal et al. [49] proposed a hybrid detection model using an SVM and a DT to identify electricity theft across energy transmission and distribution layers. The integrated DT-SVM classifier showed reliable performance in real-time theft detection. Jokar et al. [50] developed a Zigbee-based intrusion detection and prevention framework for HANs, leveraging a Q-learning-based system. This model learns optimal defense strategies through interactions with the environment, enhancing the system's ability to resist unauthorized intrusions.

Vijayanand et al. [51] implemented a multi-class SVM-based IDS aimed at detecting various attack types within the smart metering environment. Each SVM classifier was specialized to recognize a specific threat, and the system's effectiveness was evaluated using the ADFA-LD dataset. The simulation results confirmed the method's suitability for secure operation in NAN environments. Li et al. [52] presented an anomaly detection model for Advanced Metering Infrastructure (AMI) based on the Online Sequence Extreme Learning Machine (OS-ELM). Their approach aimed to enhance detection speed without sacrificing accuracy through real-time sequence training. In addition, Vijayanand et al. [53] proposed a DL-based IDS with a hierarchical architecture composed of multiple layers. The model achieved high detection rates for different types of attacks, with performance evaluated using the CICIDS 2017 dataset.

Table 5. Details for the recent IDS-based research on smart metering networks

Ref.	Year	Dataset Used	Algorithm Utilized	Network Field	Placed On	Attacks Detected	Validation Strategy	Performance Metrics
[48]	2016	KDD99	SVM and rule-based	NAN	Smart meter, data aggregation, and head-ends	DoS and probe	No	Variant for each level
[49]	2016	Custom	Fusion DT-SVM	NAN	Data aggregator	Abnormal behaviors	No	Acc=92.5%
[50]	2016	Custom	Q-learning	HAN	Smart meter	Spoofing, physical eavesdropping DoS	No	N/A
[51]	2017	ADFA-LD	Multi-SVM	NAN	Data aggregator	Exploits, DoS, fuzzers. backdoor generic, and worms	No	Acc=90%
[52]	2018	ISSDA	OS-ELM	NAN	Data aggregator	Abnormal behaviors	No	Acc=98.75%
[53]	2019	CICIDS 2017	DL and SVM	NAN	Data aggregator	DoS, PortScan, web attack. Botnet, FTP Patator and SSH Patator	No	Acc=99.99%
[54]	2020	SGCC	HDNN	NAN	Data aggregator	Electricity theft detection	No	Acc=89%
[55]	2020	SCT	SVM	NAN	Smart meter	Abnormal behaviors	Yes	Acc=98.71%
[27]	2021	KDD Cup '99 and NSL-KDD	CNN-LSTM	WAN	Head-ends	DoS, probe, R2L, and U2R	No	Acc1=99.95% Acc2 = 99.79%

Ullah et al. [54] introduced a hybrid DL model that combines CNNs and Gated Recurrent Units (GRU), optimized

using the Particle Swarm Optimization (PSO) algorithm. In this architecture, CNNs are responsible for feature extraction, while the GRU-PSO model handles classification tasks. Sun et al. [55] proposed a two-stage IDS for smart meters. In the first stage, an SVM was used to detect suspicious activities, which were then analyzed in the second stage for correlation with predefined attack patterns. The testing platform involved simulations using Network Simulator 3 and a Single-Board Computer (SBC) to emulate IEEE 802.15.4 communication between meters and the grid. Yao et al. [27] introduced a cross-layer intrusion detection model that integrates CNN and LSTM networks. The CNN-LSTM model with feature fusion was evaluated on both NSL-KDD and KDD Cup'99 datasets and outperformed conventional IDSs in terms of accuracy.

As summarized in Table 5, most of the reviewed studies have focused either on identifying specific network intrusions or detecting irregular energy consumption, but rarely both. A further limitation is the widespread reliance on outdated benchmark datasets like KDD Cup '99 and NSL-KDD, which may not fully reflect modern cyber threat landscapes. Additionally, few works have addressed the operational constraints of smart meters, such as limited processing power and memory capacity. While many proposed IDSs have demonstrated strong protection capabilities, their computational complexity may hinder practical deployment on resource-limited devices like smart meters.

4 Analysis of Review Findings

The review of existing studies on IDPS in IIoT-based smart metering networks reveals key insights into the current state of cybersecurity in industrial environments. This section summarizes the findings, highlights limitations, and identifies research gaps that must be addressed to develop an effective and scalable security solution.

4.1 Effectiveness of ML in Intrusion Detection

ML techniques have been widely adopted for intrusion detection due to their ability to recognize patterns and detect anomalies beyond traditional rule-based methods. Studies demonstrate that anomaly-based detection using ML models provides greater adaptability to emerging cyber threats than signature-based methods, which rely on predefined attack patterns. However, several challenges persist [56]:

- Many ML-based IDS solutions require high computational power, limiting their deployment on resource-constrained edge devices.
- The lack of standardized datasets for IIoT smart metering security hinders the generalizability of ML models.
- While DL models have demonstrated a high accuracy, they often require extensive training and large-scale data, which may not always be feasible in real-time IIoT environments.

4.2 Security Challenges in Smart Metering Networks

Smart metering networks form a critical component of IIoT infrastructure, yet they face multiple security threats, including [57]:

- Cyberattacks such as DoS, data falsification, and unauthorized access.
- Data privacy concerns due to the continuous transmission of consumer energy usage patterns.
- Scalability issues where increasing the number of smart meters can strain security mechanisms and cause delays in threat detection.
- Limited computational resources in edge devices that restrict the implementation of complex IDS algorithms.

4.3 Existing Approaches and Their Limitations

A comparative review of various intrusion detection methods reveals several trends [58]:

- The signature-based IDS provides quick and accurate detection for known attacks but fails to recognize novel threats.
- The anomaly-based IDS using ML techniques offers higher adaptability but often suffers from higher FPRs.
- Hybrid IDS approaches combining rule- and ML-based detection methods show promising results but require further optimization to balance accuracy and computational efficiency.
- Few studies have addressed real-time detection in smart metering networks, focusing primarily on offline data analysis rather than live threat mitigation.

4.4 Need for Adaptive and Lightweight IDPS Solutions

To address these challenges, a next-generation lightweight and adaptive IDPS is required, integrating the following features [59]:

- Resource-efficient ML models that can operate on edge devices with limited power and memory.
- Continuous model updates using online learning techniques to enhance detection capabilities over time.
- Federated learning approaches to enable collaborative anomaly detection across distributed smart metering networks without compromising data privacy.

• Integration with blockchain or distributed ledger technologies to ensure the integrity and immutability of security logs.

5 Practical Significance and Real-World Implications of Evaluation Metrics

While detection accuracy remains the most commonly reported performance metric in ML–based IDPS research, its isolated use is insufficient to evaluate practical viability in real-world IIoT smart metering environments. This section expands the result analysis by examining how core evaluation metrics—accuracy, FPR, detection latency, and computational complexity—translate into operational values when deployed in real systems.

5.1 Accuracy vs. Operational Reliability

Many of the reviewed models, particularly DL-based approaches (e.g., CNN-LSTM), report a high detection accuracy ($\geq 99\%$). However, in operational environments, high accuracy must be contextualized with system reliability:

• High accuracy with a low FPR (e.g., $< 1\%$) ensures actionable alerts and reduces alert fatigue for human operators.

• Models with high accuracy but unreported or high FPRs may lead to frequent false alarms, undermining trust and causing unnecessary mitigation responses or service disruptions.

For instance, Aydogan et al. [30] reported a 99.83% accuracy using genetic programming, but did not evaluate FPR or latency—making it unclear whether the solution is sustainable in real-time operations.

5.2 Latency and Real-Time Constraints

In IIoT smart metering, decisions must often be made in milliseconds to prevent cascading failures (e.g., fault injection or overload scenarios). However, most studies have overlooked detection latency—a critical omission:

• DL models typically require graphic processing unit (GPU) acceleration or batching, which increases latency and energy consumption.

• Lightweight models (e.g., SVM and iForest) trade off some accuracy for real-time responsiveness, making them more viable for edge deployment.

For example, Yao et al. [27] achieved a 99.95% accuracy with CNN-LSTM but did not quantify inference time. By contrast, the RealGuard system proposed by Nguyen et al. [37] prioritized edge compatibility and reported real-time detection on Raspberry Pi-class gateways.

5.3 Resource Efficiency and Edge Compatibility

Smart meters and edge gateways often have constrained resources, such as < 1 GB Random Access Memory (RAM) and limited central processing unit (CPU) cycles. Thus, the computational footprint of IDPS must align with the target device:

• Models requiring extensive training or large memory may be unsuitable for continuous edge deployment.

• Distributed or federated learning strategies (though still emerging) could offer on-device learning without centralized data exposure.

Few studies have reported memory usage or CPU load, with the exception of the study by Eskandari et al. [34], who demonstrated Passban's edge readiness on low-power gateways.

Table 6 compares selected studies across key real-world constraints.

Table 6. Comparative analysis of practical deployment features in reviewed works

Study	Accuracy	FPR Reported	Latency Reported	Edge Compatibility	Public Dataset
Axdogan et al. [30]	99.83%	No	No	Centralized only	No
Latif et al. [32]	99.20%	No	No	Moderate	Yes
Sun et al. [55]	98.71%	No	Yes (simulated)	High	Yes
Yao et al. [27]	99.95%	No	No	Low	Yes
Nguyen et al. [37]	99.64%	Yes ($< 11.5\%$)	Yes	High (Raspberry Pi)	Yes

To make ML-based IDPS deployable in IIoT smart metering networks, future work should:

• Report comprehensive metrics, including FPR, precision, recall, and latency.

• Validate models under resource-constrained settings and provide profiling data (e.g., RAM usage and inference time).

• Explore lightweight and adaptive architectures, such as federated learning, to ensure privacy and scalability.

• Benchmark against realistic traffic patterns using diverse, public datasets tailored to smart metering environments.

6 Research Gaps and Future Directions

The review findings, as shown in Table 7, suggest that while significant progress has been made in securing IIoT-based smart metering systems, the following research gaps need further exploration [60]:

• Developing real-time, low-latency intrusion detection mechanisms that can efficiently detect and mitigate threats with a minimal impact on system performance.

• Creating benchmark datasets for IIoT smart metering security to enhance model training and evaluation consistency.

• Exploring energy-efficient DL architectures that reduce computational overhead while maintaining a high detection accuracy.

• Investigating cross-domain applicability by extending IDPS solutions to other critical IIoT applications, such as smart grids and industrial automation.

Table 7. Summary of key findings

Category	Current Trends	Challenges & Gaps
Intrusion detection	ML-based anomaly detection	High false positives and resource constraints
Smart meter security	Data-driven monitoring	Privacy risks and cyberattack vulnerabilities
Computational efficiency	Lightweight ML models	Limited processing power on edge devices
Scalability & adaptability	Hybrid IDS approaches	Need for real-time and adaptive learning
Future security enhancements	Federated learning and blockchain	A lack of large-scale deployment in IIoT

7 Conclusions and Future Directions

This review presents a comprehensive and performance-driven analysis of ML-based IDPS in IIoT smart metering environments. Unlike prior surveys that focus solely on taxonomies or accuracy metrics, this study introduced a structured comparative framework that considers not only detection rates but also operational factors such as latency, resource requirements, deployment architecture, and dataset relevance. Through bar chart visualization and tabular analysis, this study demonstrated that while DL models such as CNN-LSTM achieve a high accuracy (up to 99.95%), they often lack evaluations of real-time feasibility and edge-level compatibility—critical factors in IIoT settings where devices are resource-constrained and decisions must be made in milliseconds.

Key contributions of this review include:

• A three-domain classification of existing IDPS solutions (IoT/IIoT, smart metering, and hybrid).

• A multi-metric comparison that goes beyond accuracy to assess real-world applicability.

• Identification of gaps in current research, including overreliance on outdated datasets and insufficient profiling of latency or computational load.

While a new model architecture was not proposed, the novelty of this work lies in its holistic and application-driven synthesis of prior research. The proposed benchmarking matrix offers a reference point for practitioners aiming to balance detection performance with system constraints in real deployments.

Based on the gaps identified in this study, the following avenues are recommended for future work:

a) Real-time detection optimization: Future IDPS models should prioritize latency-aware design, using techniques such as model pruning, knowledge distillation, or quantized inference to meet sub-second detection time requirements on edge devices.

b) Lightweight, resource-conscious architectures: Researchers should explore model architectures optimized for constrained hardware environments (e.g., microcontrollers and smart meters) with < 1 GB RAM and limited compute capacity.

c) Federated and continual learning: To support adaptive threat detection and privacy preservation, future systems should employ federated learning or on-device continual learning approaches that reduce dependency on centralized training and data aggregation.

d) Robust benchmarking with realistic datasets: There is a critical need for publicly available, domain-specific datasets that reflect real IIoT smart metering traffic patterns, including background noise, device heterogeneity, and attack diversity.

e) Hybrid detection strategies: Combining signature-based methods for known threats with anomaly-based ML approaches can yield more resilient detection systems, especially when paired with rule-based pre-filters or context-aware detection layers.

By incorporating these directions, the next generation of IDPS can achieve not only high detection accuracy but also practical deployability, reliability, and adaptability within the growing and complex landscape of IIoT smart metering systems.

Author Contributions

Conceptualization, Qutaiba I. Ali, Sahar L. Qaddoori; methodology, Qutaiba I. Ali, Sahar L. Qaddoori; investigation, Qutaiba I. Ali, Sahar L. Qaddoori; resources, Qutaiba I. Ali, Sahar L. Qaddoori; writing—original draft preparation, Qutaiba I. Ali, Sahar L. Qaddoori ; writing—review and editing, Qutaiba I. Ali, Sahar L. Qaddoori. All authors have read and agreed to the published version of the manuscript." The relevant terms are explained at the CRediT taxonomy.

Data Availability

The data used to support the research findings are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there is no conflict of interest in the study.

References

[1] M. K. Putchala, *Deep Learning Approach for Intrusion Detection System (IDS) in the Internet of Things (IoT) Network Using Gated Recurrent Neural Networks (GRU)*. Wright State University, 2017.

[2] Z. E. Huma, S. Latif, J. Ahmad, Z. Idrees, A. Ibrar, Z. Zou, F. Alqahtani, and F. Baothman, "A hybrid deep random neural network for cyberattack detection in the Industrial Internet of Things," *IEEE Access*, vol. 9, pp. 55 595–55 605, 2021. https://doi.org/10.1109/ACCESS.2021.3071766

[3] T. Vaiyapuri, Z. Sbai, H. Alaskar, and N. A. Alaseem, "Deep learning approaches for intrusion detection in IIoT networks–Opportunities and future directions," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 4, pp. 86–92, 2021.

[4] G. E. I. Selim, E. Hemdan, A. M. Shehata, and N. A. El-Fishawy, "Anomaly events classification and detection system in critical Industrial Internet of Things infrastructure using machine learning algorithms," *Multimed. Tools Appl.*, vol. 80, no. 8, pp. 12 619–12 640, 2021. https://doi.org/10.1007/s11042-020-10354-1

[5] X. Liu and P. S. Nielsen, "Scalable prediction-based online anomaly detection for smart meter data," *Inf. Syst.*, vol. 77, pp. 34–47, 2018. https://doi.org/10.1016/j.is.2018.05.007

[6] Q. Ibrahim and S. Lazim, "Applying an efficient searching algorithm for intrusion detection on Ubicom network processor," *Int. Arab. J. e Technol.*, vol. 2, no. 2, pp. 82–90, 2011.

[7] T. Andrysiak, L. Saganowski, and P. Kiedrowski, "Anomaly detection in smart metering infrastructure with the use of time series analysis," *J. Sens.*, vol. 2017, no. 1, p. 8782131, 2017. https://doi.org/10.1155/2017/8782131

[8] S. L. Qaddoori and Q. I. Ali, "An efficient security model for Industrial Internet of Tthings (IIoT) system based on machine learning principles," *Al-Rafidain Eng. J.*, vol. 28, no. 1, pp. 329–340, 2023.

[9] H. Qiao, J. O. Blech, and H. Chen, "A machine learning based intrusion detection approach for industrial networks," in *2020 IEEE International Conference on Industrial Technology (ICIT), Buenos Aires, Argentina*, 2020, pp. 265–270. https://doi.org/10.1109/ICIT45562.2020.9067253

[10] H. Alaiz-Moreton, J. Aveleira-Mata, J. Ondicol-Garcia, A. L. Muñoz-Castañeda, I. García, and C. Benavides, "Multiclass classification procedure for detecting attacks on MQTT-IoT protocol," *Complexity*, vol. 2019, no. 1, p. 6516253, 2019. https://doi.org/10.1155/2019/6516253

[11] Q. I. Ali, "Design and implementation of an embedded intrusion detection system for wireless applications," *IET Inf. Secur.*, vol. 6, no. 3, pp. 171–182, 2012. https://doi.org/10.1049/iet-ifs.2010.0245

[12] S. Madhawa, P. Balakrishnan, and U. Arumugam, "Roll forward validation based decision tree classification for detecting data integrity attacks in Industrial Internet of Things," *J. Intell. Fuzzy Syst.*, vol. 36, no. 3, pp. 2355–2366, 2019. https://doi.org/10.3233/JIFS-169946

[13] H. Yao, P. Gao, P. Zhang, J. Wang, C. Jiang, and L. Lu, "Hybrid intrusion detection system for edge-based IIoT relying on machine-learning-aided detection," *IEEE Network*, vol. 33, no. 5, pp. 75–81, 2019. https://doi.org/10.1109/MNET.001.1800479

[14] S. Lazim Qaddoori and Q. I. Ali, "An embedded and intelligent anomaly power consumption detection system based on smart metering," *IET Wirel. Sens. Syst.*, vol. 13, no. 2, pp. 75–90, 2023. https://doi.org/10.1049/wss2.12054

[15] N. W. Bergmann and P. J. Robinson, "Server-based Internet of Things architecture," in *2012 IEEE Consumer Communications and Networking Conference (CCNC)*, 2012, pp. 360–361.

[16] H. U. Rehman, M. Asif, and M. Ahmad, "Future applications and research challenges of IoT," in *2017 International Conference on Information and Communication Technologies (ICICT)*, 2017, pp. 68–74.

[17] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013. https://doi.org/10.1016/j.future.2013.01.010

[18] S. L. Qaddoori and Q. I. Ali, "An in-depth characterization of intrusion detection systems (IDS)," *J. Mod. Technol. Eng.*, vol. 6, 2021.

[19] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," *Comput. Netw.*, vol. 144, pp. 17–39, 2018. https://doi.org/10.1016/j.comnet.2018.07.017

[20] Q. Ibrahim and S. Lazim, "An insight review of Internet of Things (IoT) protocols, standards, platforms, applications and security issues," *Int. J. Sens. Wirel. Commun. Control*, vol. 11, no. 6, pp. 627–648, 2021. https://doi.org/10.2174/2210327910999201102194157

[21] G. S. Matharu, P. Upadhyay, and L. Chaudhary, "The Internet of Things: Challenges security issues," in *2014 International Conference on Emerging Technologies (ICET)*, 2014, pp. 54–59.

[22] Z. Song, M. T. Lazarescu, R. Tomasi, L. Lavagno, and M. A. Spirito, *High-Level Internet of Things Applications Development Using Wireless Sensor Networks*. Springer, Cham, 2014. https://doi.org/10.1007/978-3-319-04223-7_4

[23] A. Sahu, H. K. Tippanaboyana, L. Hefton, and A. Goulart, "Detection of rogue nodes in AMI networks," in *2017 19th International Conference on Intelligent System Application to Power Systems (ISAP)*, 2017, pp. 1–6.

[24] S. L. Qaddoori and Q. I. Ali, "An embedded intrusion detection and prevention system for home area networks in advanced metering infrastructure," *IET Inf. Secur.*, vol. 17, no. 3, pp. 315–334, 2023. https://doi.org/10.1049/ise2.12097

[25] A. A. Korba, N. Tamani, and Y. Ghamri-Doudane, "Anomaly-based framework for detecting power overloading cyberattacks in smart grid AMI," *Comput. Secur.*, vol. 96, p. 101896, 2020. https://doi.org/10.1016/j.cose.2020.101896

[26] S. L. Qaddoori, I. Fathi, M. A. Hammoudy, and Q. I. Ali, "Advancing public health monitoring through secure and efficient wearable technology," *Int. J. Saf. Secur. Eng.*, vol. 13, no. 6, pp. 1001–1014, 2023. https://doi.org/10.18280/ijsse.130603

[27] R. Yao, N. Wang, Z. Liu, P. Chen, and X. Sheng, "Intrusion detection system in the advanced metering infrastructure: A cross-layer feature-fusion CNN-LSTM-Based approach," *Sensors*, vol. 21, no. 2, p. 626, 2021. https://doi.org/10.3390/s21020626

[28] M. A. Khan, M. A. Khan, S. U. Jan, J. Ahmad, S. S. Jamal, A. A. Shah, N. Pitropakis, and W. J. Buchanan, "A deep learning-based intrusion detection system for MQTT enabled IoT," *Sensors*, vol. 21, no. 21, p. 7016, 2021. https://doi.org/10.3390/s21217016

[29] A. Derhab, M. Guerroumi, A. Gumaei, L. Maglaras, M. A. Ferrag, M. Mukherjee, and F. A. Khan, "Blockchain and random subspace learning-based IDS for SDN-enabled Industrial IoT security," *Sensors*, vol. 19, no. 14, p. 3119, 2019. https://doi.org/10.3390/s19143119

[30] E. Aydogan, S. Yilmaz, S. Sen, I. Butun, S. Forsström, and M. Gidlund, "A central intrusion detection system for RPL-based Industrial Internet of Things," in *2019 15th IEEE International Workshop on Factory Communication Systems (WFCS)*, 2019, pp. 1–5.

[31] A. Shalaginov, O. Semeniuta, and M. Alazab, "Meml: Resource-aware MQTT-based machine learning for network attacks detection on IoT edge devices," in *Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing Companion*, 2019, pp. 123–128.

[32] S. Latif, Z. Zou, Z. Idrees, and J. Ahmad, "A novel attack detection scheme for the Industrial Internet of Things using a lightweight random neural network," *IEEE Access*, vol. 8, pp. 89 337–89 350, 2020. https://doi.org/10.1109/ACCESS.2020.2994079

[33] M. P. Maharani, P. T. Daely, J. M. Lee, and D. S. Kim, "Attack detection in fog layer for IIoT based on machine learning approach," in *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, 2020, pp. 1880–1882.

[34] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6882–6897, 2020. https://doi.org/10.1109/JIOT.2020.2970501

[35] J. B. Awotunde, C. Chakraborty, and A. E. Adeniyi, "Intrusion detection in Industrial Internet of Things network-based on deep learning model with rule-based feature selection," *Wirel. Commun. Mob. Comput.*, vol. 2021, no. 1, p. 7154587, 2021. https://doi.org/10.1155/2021/7154587

[36] K. Raja, K. Karthikeyan, B. Abilash, K. Dev, and G. Raja, "Deep learning based attack detection in IIoT using two-level intrusion detection system," vol. 2021, pp. 1–32, 2021. https://doi.org/10.21203/rs.3.rs-997888/v1

[37] X. H. Nguyen, X. D. Nguyen, H. H. Huynh, and K. H. Le, "Realguard: A lightweight network intrusion detection system for IoT gateways," *Sensors*, vol. 22, p. 432, 2022. https://doi.org/10.3390/s22020432

[38] C. Beckel, L. Sadamori, T. Staake, and S. Santini, "Revealing household characteristics from smart meter data," *Energy*, vol. 78, pp. 397–410, 2014. https://doi.org/10.1016/j.energy.2014.10.025

[39] P. Jokar, N. Arianpoo, and V. C. Leung, "Electricity theft detection in AMI using customers' consumption patterns," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 216–226, 2016. https://doi.org/10.1109/TSG.2015.2425222

[40] S. Bhattacharjee, A. Thakur, S. Silvestri, and S. K. Das, "Statistical security incident forensics against data falsification in smart grid advanced metering infrastructure," in *Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy*, vol. 2017, 2017, pp. 35–45.

[41] J. García, E. Zamora, and H. Sossa, "Supervised and unsupervised neural networks: Experimental study for anomaly detection in electrical consumption," in *Mexican International Conference on Artificial Intelligence*, 2018, pp. 98–109.

[42] M. Xiang, H. Rao, T. Tan, Z. Wang, and Y. Ma, "Abnormal behaviour analysis algorithm for electricity consumption based on density clustering," *J. Eng.*, vol. 2019, no. 10, pp. 7250–7255, 2019. https://doi.org/10.1049/joe.2018.5123

[43] C. Chahla, H. Snoussi, L. Merghem, and M. Esseghir, "A novel approach for anomaly detection in power consumption data," in *Proceedings of the 8th International Conference on Pattern Recognition Applications and Methods (ICPRAM 2019)*, 2019, pp. 483–490.

[44] Y. Himeur, A. Alsalemi, F. Bensaali, and A. Amira, "A novel approach for detecting anomalous energy consumption based on micro-moments and deep neural networks," *Cogn. Comput.*, vol. 12, no. 6, pp. 1381–1401, 2020. https://doi.org/10.1007/s12559-020-09764-y

[45] S. V. Oprea, A. Bâra, F. C. Puican, and I. C. Radu, "Anomaly detection with machine learning algorithms and big data in electricity consumption," *Sustainability*, vol. 13, no. 19, pp. 10 963–10 982, 2021. https://doi.org/10.3390/su131910963

[46] J. Zhang, H. Zhang, S. Ding, and X. Zhang, "Power consumption predicting and anomaly detection based on transformer and k-means," *Front. Energy Res.*, vol. 9, p. 779587, 2021. https://doi.org/10.3389/fenrg.2021.779587

[47] Y. Fu, Z. Yan, J. Cao, O. Koné, and X. Cao, "An automata based intrusion detection method for Internet of Things," *Mob. Inf. Syst.*, vol. 2017, no. 1, p. 1750637, 2017. https://doi.org/10.1155/2017/1750637

[48] H. Sedjelmaci and S. M. Senouci, "Smart grid security: A new approach to detect intruders in a smart grid neighborhood area network," in *2016 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, 2016, pp. 6–11.

[49] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar, and S. Mishra, "Decision tree and SVM-based data analytics for theft detection in smart grid," *IEEE Trans. Ind. Inform.*, vol. 12, no. 3, pp. 1005–1016, 2016. https://doi.org/10.1109/TII.2016.2543145

[50] P. Jokar and V. C. Leung, "Intrusion detection and prevention for ZigBee-based home area networks in smart grids," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1800–1811, 2016. https://doi.org/10.1109/TSG.2016.2600585

[51] R. Vijayanand, D. Devaraj, and B. Kannapiran, "Support vector machine based intrusion detection system with reduced input features for advanced metering infrastructure of smart grid," in *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2017, pp. 1–7.

[52] Y. Li, R. Qiu, and S. Jing, "Intrusion detection system using Online Sequence Extreme Learning Machine (OS-ELM) in advanced metering infrastructure of smart grid," *PloS One*, vol. 13, no. 2, p. e0192216, 2018. https://doi.org/10.1371/journal.pone.0192216

[53] R. Vijayanand, D. Devaraj, and B. Kannapiran, "A novel deep learning based intrusion detection system for smart meter communication network," in *2019 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)*, 2019, pp. 1–3.

[54] A. Ullah, N. Javaid, O. Samuel, M. Imran, and M. Shoaib, "CNN and GRU based deep neural network for electricity theft detection to secure smart grid," in *2020 International Wireless Communications and Mobile Computing (IWCMC)*, 2020, pp. 1598–1602.

[55] C. C. Sun, D. J. S. Cardenas, A. Hahn, and C. C. Liu, "Intrusion detection for cybersecurity of smart meters," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 612–622, 2020. https://doi.org/10.1109/TSG.2020.3010230

[56] Q. I. Ali, "Securing solar energyharvesting roadside unit using an embedded cooperativehybrid intrusion detection system," *IET Inf. Secur.*, vol. 10, no. 6, pp. 386–402, 2016. https://doi.org/10.1049/iet-ifs.2014.0456

[57] Q. Ibrahim, "Design implementation of high-speed network devices using SRL16 Reconfigurable Content Addressable Memory (RCAM)," *Int. Arab. J. e Technol.*, vol. 2, no. 2, pp. 72–81, 2011.

[58] Q. I. Ali, "Gvanet project: An efficient deployment of a selfpowered, reliable and secured VANET infrastructure," *IET Wirel. Sens. Syst.*, vol. 8, no. 6, pp. 313–322, 2018. https://doi.org/10.1049/iet-wss.2018.5112

[59] Q. I. Ali, "Performance evaluation of WLAN internet sharing using DCF PCF modes," *Int. Arab. J. e Technol.*, vol. 1, no. 1, pp. 38–45, 2009.

[60] Q. I. Ali and J. K. Jalal, "Practical design of solar-powered IEEE 802.11 backhaul wireless repeater," in *Proceedings of the 6th International Conference on Multimedia, Computer Graphics and Broadcasting*, 2014.