International Journal on Advanced Science Engineering Information Technology

Vol.15 (2025) No. 3
ISSN: 2088-5334

Drift Management in ML-Based IoT Device Classification: A Survey and Evaluation

Quadri Waseem [a,b], Wan Isni Sofiah Wan Din [a,1], Towfeeq Fairooz [c], Ahmad Tajudin Baharin [d,2]

[a] *Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah (UMPSA), Pahang, Malaysia*
[b] *AnalytiCray, Dataran Pandan Prima, Kuala Lumpur, Malaysia*
[c] *School of Computing, Ulster University, Belfast, United Kingdom*
[d] *Faculty of Computer Science and Information Technology, University Tun Hussien Onn Malaysia, Malaysia*
Corresponding author: [1]sofiah@umpsa.edu.my; [2]tajudin@uthm.edu.my

***Abstract*—The fast-moving adaptation of the Internet of Things (IoT) and its devices has revolutionized the way we interact with connected systems and perceive the world around us. With the increasing deployment of IoT in various domains such as smart homes, healthcare, industrial automation, and intelligent transportation, ensuring the proper classification and management of IoT devices is essential. Accurate classification plays a crucial role in network management, security enforcement, Quality of Service (QoS), and overall system performance optimization. However, the dynamic nature of IoT environments presents a significant challenge for effective IoT device classification, specifically in the form of drift. Drift occurs when device characteristics and behaviors change over time, making it challenging to maintain accurate classification. This issue is particularly prevalent in applications like smart homes, smart infrastructures, smart cities, and industrial IoT, where diverse and evolving devices contribute to data variability and uncertainty. This survey examines the application of machine learning techniques in mitigating drift in IoT device classification, with a focus on prevention, detection, adaptation, and mitigation strategies. Additionally, we discuss the open challenges and limitations of existing machine learning (ML)-based models used for drift management, as well as future research directions. By analyzing the current landscape of drift management in IoT, this research survey provides valuable insights. It highlights critical gaps that need to be addressed for more robust and efficient IoT classification models.**

***Keywords*— Drift management; machine learning; IoT device classification.**

Manuscript received 8 Oct. 2024; revised 11 Feb. 2025; accepted 17 Apr. 2025. Date of publication 30 Jun. 2025.

I. Introduction

The Internet of Things (IoT) has emerged in a new era where smart IoT devices are an integral part of our daily lives, spanning from smart homes to smart cities and finally moving towards large-scale industries and infrastructures. These smart IoT devices extend their influence even further into areas like construction, healthcare, transportation, and beyond [1]. Effective and efficient classification of these IoT devices is essential for network management (NM), security, QoS and performance optimization. However, the dynamic nature of the IoT ecosystem presents a persistent challenge known as" drift" [2], which is a nuanced phenomenon characterized by a gradual shift in data distribution away from the original patterns [3] because of a variety of factors, including firmware updates, network changes, and the addition of new IoT devices [4]. While these updates are essential for enhancing device functionality and security, they simultaneously introduce changes in device behavior and data traffic patterns, rendering machine learning (ML) classification less accurate. Furthermore, the continuous release of new device versions, each with unique features and communication methods, adds complexity to the classification task [5]. With each new iteration, the data characteristics evolve, exacerbating the challenge of concept drift [6]. Additionally, IoT devices operate within network environments characterized by inherent variability, leading to fluctuations in data traffic patterns and intensifying the concept of drift. The repercussions of concept drift extend throughout the IoT ecosystem, impacting every layer of device classification severely [7].

In case of IoT device classification, machine learning models are always fine-tuned for accuracy and performance [8]. However, drift can lead to a decline in accuracy, which is detrimental and unacceptable for security-focused applications [9]. Misclassifications resulting from concept drift can expose vulnerabilities that malicious actors exploit, jeopardizing user privacy, security, and organizational integrity. Moreover, the operational efficiency of IoT applications becomes increasingly vulnerable to disruption as machine learning (ML) models struggle to adapt to shifting data distributions. These disruptions introduce significant complexity and necessitate retraining, which is concerning in terms of both time and cost. In response to these multifaceted challenges introduced by concept drift, ML models have evolved, adapted, and emerged as a pivotal solution [10]. These models possess the innate capacity to evolve and recalibrate their decision boundaries, accommodating the changing characteristics and behaviors of IoT devices. Through continuous learning from newly generated data, these dynamic models exhibit the resilience required to navigate the intricacies and dynamism of the ever-evolving IoT landscape.

Hence, this research embarks on a comprehensive exploration of drift management within the realm of IoT device classification from a machine learning (ML) perspective. It aims to explore a wide range of methodologies, techniques, and strategies for preventing, detecting, adapting to, and mitigating drift issues. This extensive study provides invaluable insights into drift management through an evaluative analysis of various machine learning (ML) based algorithms for IoT device classification. By managing the drifts, this research aims to elevate the security, performance, and efficiency of IoT systems in real-world scenarios, thereby facilitating the seamless and secure integration of IoT devices into our interconnected world.

A. Research Questions and Motivation

1) RQ1: How can a machine learning technique effectively manage drift in IoT device classification?

Motivation Behind: The aim is to identify and evaluate the various ML techniques through previously published research and mention the important components of drift management and their ML utilization.

*2) RQ2***:** What are the practical challenges and potential future directions in addressing concept drift management, covering drift detection, adaptation, and mitigation in IoT device classification?

Motivation Behind: This research also aims to identify the main challenges of existing drift management and its components. The various concepts discussed here will aid in identifying future research areas for the prevention, detection, adaptation, and mitigation of drift.

*3) RQ3***:** What are the research gaps in the field of drift management in the context of machine learning-based IoT device classification?

Motivation Behind: The aim is to identify the research gaps at each level of the component of drift management so that in the future, we can avoid the drift at an early stage.

B. Contributions

The contribution of this study includes:

a. This research explores the use of machine learning techniques to manage drift management in IoT device classification, encompassing drift prevention detection, drift adaptation, and drift mitigation.
b. To study and discuss the practical open issues and challenges of various ML-based models, along with future directions in the context of managing concept drift for IoT device classification.
c. To investigate and evaluate the critical analysis for research gaps of drift management and its components in ML-based IoT device classification.

This research aims to investigate the application of machine learning methods for comprehensive management of concept drift in IoT device classification, focusing on drift prevention, detection, adaptation, and mitigation techniques. It addresses the practical challenges and prospects in real-world IoT applications.

C. The Structure of this Study

The structure of this study outlines how drift management is controlled and managed. In terms of various sections and sub-sections, it provides more details for the readers. Overall, this research paper serves as a guide to help readers navigate and open the hidden doors of drift management regarding IoT device classification effectively and efficiently.

This research paper includes sections as mentioned in Figure 1, which include an introduction, related surveys, methodology, machine learning (ML) algorithms for IoT device classification, drift and its effects on IoT classification, comparison analysis and evaluation, challenges of drift management, critical gap analysis, discussion and suggestions, future direction of drift management and conclusion.

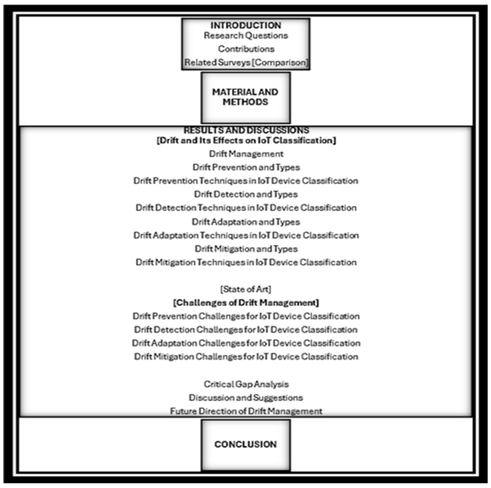

INTRODUCTION
Research Questions
Contributions
Related Surveys [Comparison]
MATERIAL AND METHODS
RESULTS AND DISCUSSIONS
[Drift and Its Effects on IoT Classification]
Drift Management
Drift Prevention and Types
Drift Prevention Techniques in IoT Device Classification
Drift Detection and Types
Drift Detection Techniques in IoT Device Classification
Drift Adaptation and Types
Drift Adaptation Techniques in IoT Device Classification
Drift Mitigation and Types
Drift Mitigation Techniques in IoT Device Classification
[State of Art]
[Challenges of Drift Management]
Drift Prevention Challenges for IoT Device Classification
Drift Detection Challenges for IoT Device Classification
Drift Adaptation Challenges for IoT Device Classification
Drift Mitigation Challenges for IoT Device Classification
Critical Gap Analysis
Discussion and Suggestions
Future Direction of Drift Management
CONCLUSION

Fig. 1 Paper Structure

D. Related Survey

Several studies have been proposed related to drift management. However, to our understanding, we did not find any related research similar to this one. Here, we provide a comprehensive systematic review of drift management, covering all key aspects of drift prevention, detection, adaptation, and mitigation in detail, along with an evaluation, valuable insights, and a detailed analysis of challenges and gaps. The review also includes discussions and suggestions for the future. Some of these works are presented in Table 1 and are also compared with this research work.

TABLE I

RELATED SURVEYS AND COMPARISON

Ref.	Year	Description	Concepts Addressed	Comparison with Our Work
[11]	Year 2020	The objective of this work is more towards a systematic literature review of existing concepts of drift detection methods on unlabeled data streams	Covers various aspects, focusing on the learning process and the way concept drift is monitored in the data stream mining models	Our research extends the insights; we focus specifically and more on IoT device classification and streams in a broader vision
[12]	Year 2022	The objective of this work is more towards evaluating performance-based methods for detecting drift in Predictive Systems	Covers review, taxonomy, and literature	Our research explores more than the detection of drift management, including other aspects besides detection
[13]	Year 2022	The objective of this work is to focus on the active and passive concepts of drift handling methods	It covers the classification of drift handling methods, compares algorithms, and provides drift types, Advantages, and disadvantages	Our research complements this by providing more details on all pillars of drift management, not only active and passive classification
[14]	Year 2023	The objective of this work is more towards drift detection in unlabeled data streams only	It covers a literature review, adapts and detects concepts along with challenges and performance Metrics, ML approaches, new research trends, and future research directions were discussed	Our research offers detailed insights into overall drift management, not only detecting, but also filling a gap in the literature via gap analysis and discussion
Year 2024	Our Survey	We analyze IoT device classification drift challenges, and present a cutting-edge drift management analysis comprehensive review tailored to IoT device classification	The objective of this work is more toward a comprehensive review, along with an evaluation	Our research offers IoT drift management via its four essential components. It also provides IoT-specific drift solutions and complete insights for challenges, gap analysis, and future direction

II. MATERIALS AND METHOD

The research methodology employed in this paper consists of two distinct review strategies. The first review strategy entails conducting a systematic literature review to identify, evaluate, and interpret influential studies within the specific area of interest of IoT device classification. This systematic literature review primarily aimed to synthesize recent and pertinent academic literature and assess the current research landscape of ML based IoT device classification. It facilitated the extraction of key findings from published works related to the research study at hand.

The second strategy was to explore the various papers related to "drift detection,"" drift adaptation," drift mitigation, "drift prevention,"" ML and Drifts," as well as" Machine Learning and Drifts". To collect our research papers, we accessed various respected academic databases such as Scopus, Elsevier, and IEEE, as well as various other online resources and academic journals related to ML, IoT classification, and drift. We initiated our search by collecting 30 papers using diverse search engines. After eliminating duplicates, we were left with 20 distinct research articles. Next, we performed an in-depth review of the abstracts to ensure that the selected papers aligned with our research objectives. Basic review articles and those not directly related to "IoT and Drift" were excluded from our final selection. This careful curation process resulted in the inclusion of 14 research articles, which form the core of our investigation. The paper selection process is illustrated in Figure 2, which provides a clear overview of our meticulous data-gathering approach.

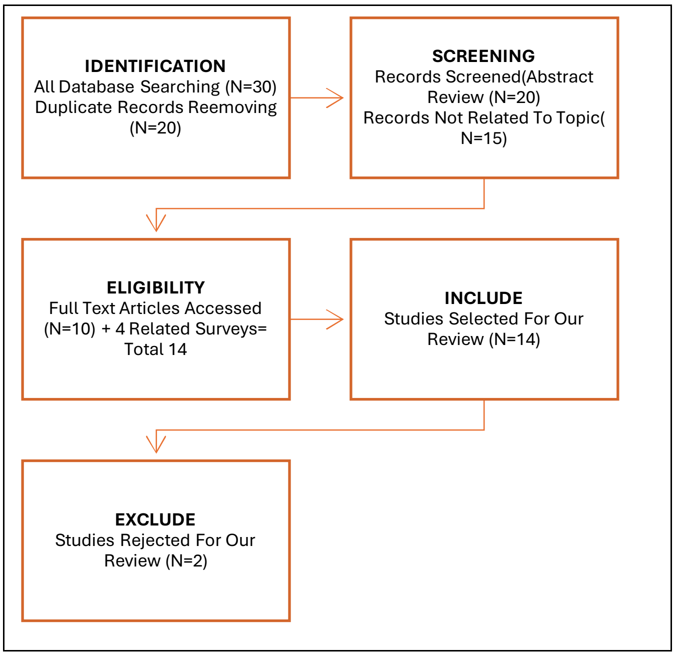

IDENTIFICATION
All Database Searching (N=30)
Duplicate Records Reemoving (N=20)
SCREENING
Records Screened(Abstract Review (N=20)
Records Not Related To Topic(N=15)
ELIGIBILITY
Full Text Articles Accessed (N=10) + 4 Related Surveys= Total 14
INCLUDE
Studies Selected For Our Review (N=14)
EXCLUDE
Studies Rejected For Our Review (N=2)

Fig. 2 Methodology Used

III. RESULTS AND DISCUSSION

Machine learning (ML) algorithms for IoT device classification are trained on datasets containing features extracted from IoT device data, allowing them to learn patterns and make predictions about the device's class. Various machine learning (ML) algorithms, including supervised learning, unsupervised learning, and deep learning, can be applied to tackle IoT device classification challenges [15]. Supervised ML algorithms like neural networks, decision trees, and support vector machines (SVM) are commonly employed. Particularly, deep learning (DL) models stand out for their ability to automatically learn relevant features from raw data. Decision trees are prized for their interpretability, while SVMs excel in dimensional spaces and complex decision boundaries. Hybrid techniques combining K-Means clustering and SVM can be valuable for concept drift detection in network anomaly detection [16]. Unsupervised learning algorithms, such as clustering methods and anomaly detection, prove their worth when labeled data is limited. Clustering methods like K-Means and hierarchical clustering group similar IoT devices based on data patterns, aiding in identifying common characteristics, while anomaly detection techniques are crucial for maintaining IoT network security [17]. Semi-supervised learning and active learning bridge the gap between labeled and unlabeled data, offering cost-effective solutions and intelligent data selection for labeling, respectively [18]. Lastly, transfer learning is leveraged when dealing with limited labeled data, allowing for the fine-tuning of pre-trained models for specific IoT classification tasks. Clustering methods, as mentioned earlier, remain valuable for grouping devices with similar characteristics in scenarios where labeled data is scarce [19]. Hence, Figure 3 illustrates the taxonomy of machine learning (ML) for IoT device classification.

A. *Drift and Its Effect on IoT Device Classification*

Drift in IoT device classification refers to the changing statistical characteristics of data over time, which can challenge the accuracy of classification models. In IoT environments, device behaviors can evolve due to firmware updates, changes in user behavior, or malfunctions. Formally, the concept of drift between two points at time instants t = 0 and t = 1, respectively, can be defined as Eq. (1) [20], in which pt = 0 is the coexisting distribution of the input variable X and the target variable y at time t = 0.

$$\exists X : pt=0(X,y)\ ,\ pt=1(X,y) \qquad (1)$$

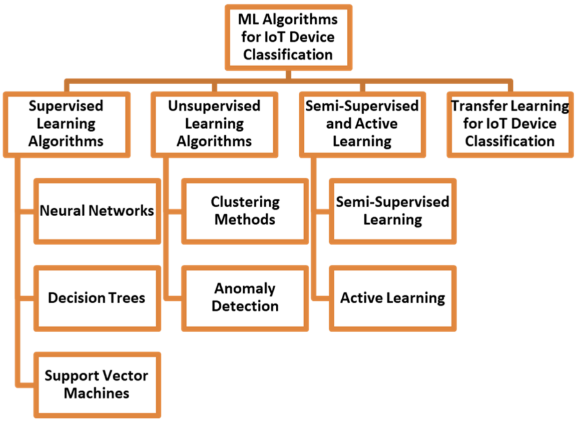

ML Algorithms for IoT Device Classification
Supervised Learning Algorithms
Unsupervised Learning Algorithms
Semi-Supervised and Active Learning
Transfer Learning for IoT Device Classification
Neural Networks
Decision Trees
Support Vector Machines
Clustering Methods
Anomaly Detection
Semi-Supervised Learning
Active Learning

Fig. 3 Taxonomy of ML for IoT Device Classification

The data shows less variation, indicating no drift values, within the range of 2-4 on the variation axis. However, sudden changes over time are apparent from the range of 4 to 6 on the variation axis, indicating drift values. Figure 4 illustrates the drift problem.[21], hence continuous detection/monitoring, adaptation, mitigation and the development of robust, real-time machine learning algorithms are essential to deal with the issue. These algorithms should detect and respond to concept drift, ensuring that IoT devices can be accurately identified and classified, even as their behaviors change, thereby maintaining the effectiveness of security and management systems in IoT ecosystems [22].

Concept drift occurs when the joint probability distributions between input data x and outcomes y at two different times, denoted as $P_{t=0}$ and $P_{t=1}$, are not equal, as shown by the equation $P_{t=0}(x,y)$, $P_{t=1}(x,y)$. Additionally, suppose the product of the probability of x and the conditional probability of y given x, Pt(x)Pt(y|x), is not equal between the two-time points. In that case, concept drift also occurs, which is represented by Eq. (2).

$$P_{t0}(x)P_{t0}(y|x)\ ,\ P_{t1}(x)P_{t1}(y|x) \qquad (2)$$

These changes can be categorized into virtual concept drift, where only the probability of x changes; real concept drift, where only the conditional probability of y given x changes; and hybrid concept drift, where both occur simultaneously [23].

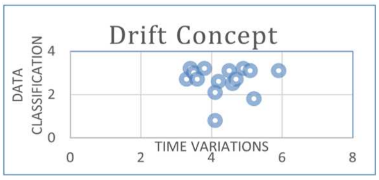


Fig. 4 Drift In IoT Classification

B. *Drift Management*

Drift management involves the comprehensive handling of drift-related challenges in the era of machine learning. Drift prevention is the proactive first stage and step in issue management, aimed at minimizing the likelihood of issues before they occur. It involves designing systems and protocols to reduce risks. It is essential for system reliability in dynamic environments, laying the foundation for post subsequent stages like drift detection, adaptation, and mitigation stages to ensure that models remain accurate and reliable in dynamic data environments [24].

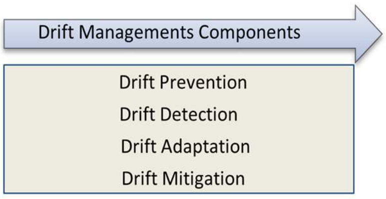


Fig. 5 Drift Management Components

Effective drift management aims to minimize the impact of drift events, reduce the frequency of adaptations, and proactively maintain model stability, ultimately contributing to the overall performance and resilience of machine learning systems, especially in applications like IoT device classification [25]. Various drift management components in IoT device classification are presented in Figure 5, which include drift prevention, drift detection, drift adaptation, and drift mitigation.

1) *Drift Prevention and Types:*

In the context of IoT device classification, drift prevention is the proactive endeavor to mitigate the occurrence of concept drift (a phenomenon where data characteristics from IoT devices change over time). These changes can manifest gradually or suddenly due to various factors, including device aging, firmware updates, environmental variations, or malicious activities. Drift prevention plays a crucial role as a pre-stage in maintaining the stability and performance of machine learning models utilized for IoT device classification. It focuses on proactively implementing strategies to reduce the likelihood of these unwanted changes taking place, safeguarding the accuracy and consistency of the models [26].

Drift prevention encompasses several distinct forms in the form of types, each tailored to address specific types of drift. First, there are Proactive strategies for mitigating concept drift, which aim to anticipate and mitigate changes in the fundamental concepts that a model captures over time. For instance, in the context of a smart home, where devices may have seasonally changing behavior, proactive adaptation strategies can help maintain model accuracy. Second, Preventive approaches for contextual Shift involve measures to counter variations in contextual factors related to IoT devices. These contextual changes may include shifts in location or user preferences, which can impact the performance of devices like wearable fitness trackers. Finally, the measures to ensure data value stability focus on measures to minimize fluctuations in the scale or magnitude of data values [27], [28]. Consider sensor readings from IoT devices that may experience variations in magnitude due to external factors; drift prevention strategies can be put in place to ensure stable data collection and accurate model performance. Hence, drift prevention is pivotal in the realm of IoT device classification, helping to proactively safeguard the integrity of machine learning models and the reliability of IoT applications by minimizing the chances of concept drift occurrences [29].

2) Drift Prevention Techniques in IoT Device Classification:

Drift prevention methods in IoT device classification encompass a distinct set of approaches and strategies aimed at proactively reducing the likelihood of concept drift occurrences. These techniques are fundamentally different from drift detection measures and are crucial for establishing robust and resilient machine learning models [30]. Several preventive strategies that can be employed are as follows:

- Model Maintenance and Continuous Training.
- Model Generalization and Feature Engineering.
- Data Quality Control.
- Change Management.

Model maintenance and continuous training refer to regularly updating and retraining machine learning models with new and relevant data. It helps prevent models from becoming outdated and less accurate over time. Developing a generalized model that can adapt to changing scenarios and work with various updated features is crucial. Careful feature selection and feature engineering can lead to more stable and less sensitive models, thereby effectively reducing the risk of concept drift. Even with new additions of IoT devices or network changes, opting for no change in the existing ML model training or updated training can maintain model stability.

Implementing rigorous data quality control measures is essential to ensure the consistency and reliability of training data. This reduces the chances of unwanted shifts and helps prevent drift-related issues from occurring. Establishing thorough change management protocols can help manage firmware updates, system modifications, and other potential sources of concept drift, ensuring they are well-controlled and tested before implementation. Anomaly Detection: Employing anomaly detection techniques can help identify unexpected deviations in data patterns, allowing for immediate action to be taken to prevent drift.

These preventive techniques play a vital role in preserving the accuracy and reliability of machine learning models in IoT device classification. By proactively addressing potential sources of drift and maintaining the quality of data and models, these strategies contribute to the long-term success of IoT applications.

3) Drift Detection and Types:

In the context of IoT device classification, drift refers to the phenomenon where data characteristics from IoT devices change over time. These changes can occur gradually or abruptly due to factors like device aging, firmware updates, environmental variations, or malicious activities. Drift detection holds immense importance as it ensures the continued performance and reliability of machine learning models used for IoT device classification. Drift detection involves identifying changes or shifts in data patterns over time. It enables these models to adapt to evolving data patterns and make accurate predictions [31].

Detecting drift in IoT data is crucial for maintaining the accuracy and reliability of models, and it encompasses several distinct forms, categorized into types [32]. First, there's Concept Drift, which arises when the very essence of what a model seeks to capture evolves. Take, for example, a smart thermostat in a household setting; its behavior may shift seasonally, necessitating an adaptable model. Second, Context Drift involves alterations in contextual factors associated with IoT devices, such as changes in location or user preferences. This type of drift can impact the performance of devices like wearable fitness trackers, which may adjust their behavior based on a user's current location and activities. Lastly, Magnitude Drift highlights fluctuations in the scale or magnitude of data values, indicating potential drift [33], [34]. Consider sensor readings from an IoT device that may vary in magnitude due to various external factors, underscoring the need for robust drift detection methods that can address these diverse manifestations of data drift.

4) Drift Detection Techniques in IoT Device Classification:

Drift detection methods in IoT device classification vary in complexity and approach. Standard techniques include statistical, ensemble, and change point detection methods. Statistical methods utilize and analyze the statistical properties of data, including the mean, distribution, and variance, to detect drift. Machine Learning Models: ML models can be trained to classify data instances as belonging to the current concept or showing drift.

Ensemble methods encompass combining multiple drift detectors to enhance detection accuracy and robustness. At the same time, change point detection focuses on identifying abrupt changes in data patterns, which may signal a drift. The two common techniques for detecting concept drift are ADWIN and DDM. ADWIN is a distribution-based method that uses an adaptive sliding window to detect the drift issue based on data distribution changes. Once a drift point is detected, all old data samples before that point are discarded.

DDM is a very famous model performance-based method that utilizes two thresholds to monitor a model's standard deviation changes and error rate for drift detection. While ADWIN is very effective at detecting gradual drifts, DDM is better suited for sudden drifts. However, DDM's response time can be slow for gradual drifts, and memory overflows can occur due to the large number of data samples needed to reach the drift level of a long gradual drift [35].

5) *Drift Adaptation and Types:*

During IoT device classification, drift adaptation is a critical concept and must be preplanned. Drift, which signifies the evolving characteristics of data from IoT devices over time, necessitates adaptation in machine learning models. Drift adaptation refers to the actions taken in response to detected drift to ensure that machine learning models remain accurate and reliable. These adaptations are crucial for maintaining accuracy [36]. And the reliability of classification models in the face of changing data patterns [37]. Effective drift adaptation ensures that models can seamlessly adjust to new conditions and continue to make precise predictions [27].

In IoT device classification, adapting to drift encompasses a range of strategies tailored to the specific characteristics of the encountered [37]. Various types of drift adaptation include, First, Model Update involves revising the classification model when the fundamental data concept shifts, accommodating changes such as seasonally evolving behavior in smart home devices. Second, Dynamic Parameter Tuning adjusts model parameters in real-time to address drift, as exemplified by wearable devices that modify classification thresholds in response to shifting user activity. Third, Ensemble Techniques combine multiple models or detectors, leveraging their strengths with weighted contributions for enhanced adaptability. Lastly, Reactive Strategies respond to detected drift with immediate actions, such as switching to alternate classifiers when the primary one becomes ineffective, ensuring continual and accurate classification in the dynamic landscape of IoT environments.

6) *Drift Adaptation Techniques in IoT Device Classification:*

Several techniques are employed for drift adaptation in IoT device classification. The first technique is reactive model updates. When drift is detected, the model is retrained or updated to accommodate the new data concept. The second technique is threshold adjustments. Classification thresholds can be dynamically adjusted based on data changes, enabling real-time adaptation. The following technique is an ensemble that combines multiple models or drift detectors to improve adaptation performance. Finally, automated machine learning methods can facilitate the adaptation process by autonomously reconfiguring models.

7) *Drift Mitigation and Types:*

Drift mitigation is a vital component in IoT device classification, addressing the challenges posed by evolving data patterns over time. It takes a proactive stance, extending beyond detection and adaptation, to ensure the ongoing stability, accuracy, and reliability of classification models. By implementing strategies such as enhancing data quality, optimizing feature engineering, selecting robust algorithms, and designing systems resistant to drift, drift mitigation significantly reduces the frequency and severity of drift events [38]. This proactive approach yields a machine learning system that maintains high accuracy with fewer adaptations, making it particularly valuable in dynamic environments, such as IoT device classification [39].

Drift mitigation in IoT device classification encompasses a range of proactive strategies to enhance system resilience. Various types of drift mitigation include, First, Data Quality Enhancement focuses on improving data quality and reliability to minimize the occurrence of drift. Second, Feature Engineering involves crafting robust features that are less affected by data changes. Third, Robust Algorithm Selection entails choosing algorithms that are less sensitive to evolving data patterns. Lastly, Inherent Drift Resistance involves designing systems inherently resilient to drift, ensuring a dependable classification process in dynamic IoT environments.

8) *Drift Mitigation Techniques in IoT Device Classification:*

Techniques employed for drift mitigation in IoT device classification include proactive strategies like:

a. Pre-emptive Model Updates: Updating models proactively to align with evolving data patterns.
b. Adaptive Thresholds: Dynamically adjusting classification thresholds based on data changes.
c. Ensemble Approaches: Combining multiple models or drift detectors to enhance mitigation.
d. Automated Mitigation: Leveraging automated machine learning methods to reconfigure models autonomously.

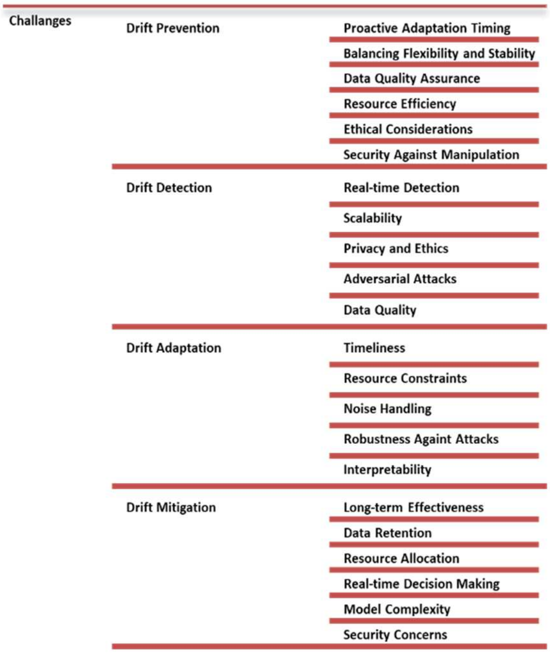
C. State of the Art for Drift Management (Detection, Adaptation, and Mitigation) using ML

Table II summarizes various works of machine learning drift techniques and their applications in different domains, offering several key insights. Firstly, many of these techniques are computationally intensive and resource demanding, potentially impacting their practicality due to increased complexity and computational costs. Additionally, the performance of these methods heavily relies on the quality of data and the suitability of base models. Furthermore, while some drift detection techniques reduce the need for manual intervention, complete elimination may not be achievable, particularly when statistical expertise is required. Finally, computational complexity poses challenges in IoT intrusion detection, where resource constraints are typical. Also, we have seen that fewer initiatives are taken to deal with the drifts before they exist, as in the case of drift prevention.

We further discuss challenges and future directions for managing drift in IoT device classification. Drift, a significant challenge in this field, arises due to the dynamic nature of IoT environments, where devices exhibit evolving behaviors over time. Key concerns include developing adaptable classification models, ensuring scalability to handle large datasets, addressing privacy considerations, and mitigating ethical implications. Security is paramount, given the vulnerability of IoT devices to malicious attacks and the threat posed by adversarial machine learning. Robust models that can handle noisy and incomplete data are needed. Specific challenges, including drift prevention, detection, adaptation, and mitigation, are presented in Figure 6.

TABLE II
EXISTING ML WORK RELATED TO DRIFT TECHNIQUES (ALL)

Works	Drift Management	Drift Handling Technique	Purpose and Domain	Advantages	Disadvantages
2022 [40]	Adaptation	Uses Random Forests (RFs) to accommodate drift effectively	Security purpose for smart IoT and Non-IoT device classification	Frequently updated for high performance. The original model is rebuilt only when data drift is detected	Each addition of new devices requires updates, increasing complexity and computational cost
2021 [41]	Adaptation	Uses Weighted Probability Averaging Ensemble (PWPAE) framework to control drift	Adaptive IoT anomaly detection via IoT data stream and analytics	Improved weighting function. Strong robust ensemble model	Performance heavily depends on well performing base learners. Limited scalability for large datasets. Performance may be affected by fluctuating real-time error rates
2017 [42]	Detection	Utilizes statistical comparison of samples for drift identification	Malware Classification Models	Statistical significance. A better understanding of model generalization	More stress toward drift detection only. Manual intervention may be required. Statistical expertise needed
2023 [43]	Detection	Utilizes Lightweight Ensemble of Data Drift Detectors (LE3D1)	Identify data irregularities in sensor stream	Lightweight and minimal overhead. Dynamic adaptation	Limited to two-tier hierarchical fashion. Limited information on approach
2022 [44]	Detection and Mitigation	Device identification using IPFIX to minimize data	Detect devices posing security risk	Minimizes data sent for identification. Handles concept drift	Concept drift in some devices may affect accuracy
2019 [45]	Adaptation	Handles demand drift through adaptive learning	IoT resource management	Reduced energy consumption and response time. Better results under heavy traffic	Complexity and resource-intensive implementation. Overfitting, privacy, and security concerns
2021 [46]	Adaptation	Novel feature selection method based on feature drift	Device Identification	Enhanced accuracy and robustness	Slow searching algorithms
2019 [47]	Detection and Adaptation	Employs improved Linear Four Rates (LFR) method for concept drifts	Condition-Based Maintenance (CBM) for smart factories	Improved accuracy. Compatible with existing offline classifiers	Performance depends on data sampling
2022 [48]	Detection and Adaptation	Comprehensive solution for detecting and mitigating drift	Intrusion detection	Reduced FP and FN. It requires processing power and longer execution times	Performance may vary
2021 [49]	Detection and Adaptation	Optimized Adaptive and Sliding Windowing (OASW) framework	Anomaly detection	Efficient addressed drift. High accuracy, low resource usage	Longer execution times. Performance variation in different IoT applications
2023 [50]	Adaptation	Integrates active and passive adaptation strategies without requiring a predefined drift threshold	Load forecasting in energy management systems (EMS) to optimize energy scheduling and enable intelligent power grids	Improves prediction performance without drift threshold setting	Computational cost trade-off with prediction accuracy
2022 [51]	Detection and Adaptation	Learns fraudulent transactions incrementally to adapt to real-time drifts	Credit card fraud detection in online transactions with concept drift	Improves fraud detection performance over time	Improves fraud detection performance over time
2023 [52]	Detection and Adaptation	Detects and adapts to concept drift in network anomalies	Network anomaly detection in cybersecurity	Effective in detecting different types of drift and enhancing anomaly detection	Computationally expensive due to the hybrid model and requires tuning
2024 [53]	Mitigation	Federated fuzzy c-means clustering and federated fuzzy Davies-Bouldin index	Federated learning (FL) for data drift detection	Detects global data drifts while preserving data privacy	Sensitive to parameter choices
2024 [54]	Detection and Mitigation	Detects harmful drift using Data Distributions with Low Accuracy (DDLA) before retraining	Machine learning (ML) pipeline optimization	Reduces unnecessary retraining and enhances cost	Relies on decision tree interpretation and may not detect all types of harmful drift



Challanges		
	Drift Prevention	Proactive Adaptation Timing
		Balancing Flexibility and Stability
		Data Quality Assurance
		Resource Efficiency
		Ethical Considerations
		Security Against Manipulation
	Drift Detection	Real-time Detection
		Scalability
		Privacy and Ethics
		Adversarial Attacks
		Data Quality
	Drift Adaptation	Timeliness
		Resource Constraints
		Noise Handling
		Robustness Againt Attacks
		Interpretability
	Drift Mitigation	Long-term Effectiveness
		Data Retention
		Resource Allocation
		Real-time Decision Making
		Model Complexity
		Security Concerns

Fig. 6 Challenges of Drift Management

D. Drift Prevention Challenges for IoT Device Classification

Preventing drift in IoT device data presents several challenges, which include:

a. Proactive Adaptation Timing: Preventing drift necessitates predicting when changes might occur and implementing preventive measures ahead of time. Timing these adaptations proactively without overreacting is a challenge.

b. Balancing Flexibility and Stability: Drift prevention strategies should maintain model stability while allowing for adaptation to changing circumstances. Striking the right balance between flexibility and stability is a complex task.

c. Balancing Flexibility and Stability: Ensuring that incoming data is of high quality and free from anomalies is essential for effective drift prevention. Quality control mechanisms must be in place to handle noisy or incomplete data.

d. Resource Efficiency: Drift prevention should be resource-efficient, especially in resource-constrained IoT environments. Ensuring that preventive measures do not overly tax device resources is a challenge.

e. Ethical Considerations: Implementing preventive measures might involve monitoring user behavior and device data. Balancing the need for drift prevention with user privacy and ethical considerations is a crucial challenge.

f. Security Against Manipulation: Drift prevention strategies must safeguard against potential manipulation by malicious actors who may attempt to induce drift or circumvent preventive measures. Ensuring robust security against such threats is a significant challenge. These challenges in drift prevention are critical in the context of IoT device classification to maintain model stability and reliability while proactively addressing the risk of concept drift.

E. Drift Detection Challenges for IoT Device Classification

Detecting drift in IoT device data presents several challenges, which include:

a. Real-time Detection: IoT systems often require real-time or near-real-time detection of drift for prompt responses. Developing drift detection methods that can operate in time-sensitive environments is a challenging task.

b. Scalability: With the increasing number of IoT devices, scalable drift detection solutions are essential to handle large volumes of streaming data efficiently.

c. Privacy and Ethics: Drift detection may involve monitoring user behavior and device data. Balancing the need for drift detection with user privacy and ethical considerations is crucial.

d. Adversarial Attacks: Malicious actors can manipulate IoT data to trigger false alarms or evade detection. Drift detection methods must be resilient to such adversarial attacks.

e. Data Quality: Noisy or incomplete data can make it challenging to distinguish genuine drift from data anomalies. Robust drift detection mechanisms are needed to handle data quality issues.

F. Drift Adaptation Challenges for IoT Device Classification

Drift adaptation in IoT device classification encounters specific challenges, which include:

a. Timeliness: Adaptations must occur promptly to maintain model accuracy. Delayed adaptations may lead to incorrect classifications.

b. Resource Constraints: IoT devices often have limited computational resources. Adapting complex models with minimal resources is a challenge.

c. Noise Handling: Drift adaptation methods must distinguish between genuine drift and random noise or anomalies in data.

d. Robustness Against Adversarial Attacks: Adversaries can exploit adaptations to deceive models. Drift adaptation strategies must be resilient against such attacks.

e. Interpretability: Ensuring that adapted models remain interpretable and explainable is important for transparency and trust.

G. Drift Mitigation Challenges for IoT Device Classification

Mitigating drift in IoT device classification presents specific challenges, which include:

a. Long-term Effectiveness: Mitigation strategies must address the long-term consequences of concept drift to ensure sustained model accuracy over time.

b. Data Retention: Maintaining a historical record of data becomes crucial to assessing and mitigating the impact of concept drift accurately.

c. Resource Allocation: Allocating sufficient resources for continuous model improvement and mitigation strategies can be challenging within resource-constrained IoT environments.

d. Real-time Decision-making: Swift and accurate decisions are required to adapt to drift and mitigating the effects in real time can be complex.

e. Model Complexity: Balancing the complexity of mitigation models with the resource limitations of IoT devices is an ongoing challenge.

f. Security Concerns: Ensuring that mitigation measures do not inadvertently introduce vulnerabilities or expose the system to security risks is a critical consideration.

H. Critical Gap Analysis

This critical analysis focuses on the specific challenges and research gaps concerning the issue of drift in IoT device classification. Drawing insights from the comprehensive evaluation, we shed light on the critical concerns related to drift prevention, drift detection, drift adaptability and drift mitigation based on their specific challenges in the context of machine learning (ML) classification for IoT devices. In our in-depth analysis of research gaps for IoT device classification, particularly concerning the pervasive challenge of drift. It is observed that:

1) For Drift Challenges in IoT Device Classification: There are 21 distinct challenges identified across these areas. A total of 21 distinct challenges are identified, which include (6 Prevention +5 Detection +5 Adaptability +5 Mitigation) challenges are discussed here, and several critical lessons have emerged to shape future endeavors in this domain.

2) For Scalability and Resource Efficiency: With the growth of IoT deployments, scalable solutions accommodating device proliferation and drift complexities are essential. Resource-efficient solutions are necessary for resource-constrained environments.

3) For Data-Driven Approaches: Developing techniques leveraging unlabeled data for drift detection can enhance classification accuracy.

4) For Security and Privacy Measures: Drift detection and adaptation mechanisms must withstand potential attacks and protect sensitive IoT data integrity.

5) For Critical Insights for Future Research

a. Swift prevention and detection of drift are crucial for maintaining classification model accuracy.

b. Real-time detection and proactive adaptation are necessary, supported by suitable ML algorithms.

c. Standardization of ML models and algorithms is essential for compatibility and interoperability in diverse IoT setups.

d. Model generalization is vital for long-term accuracy improvement and resilience against drifting.

e. Adaptive strategies balancing stability and adaptability are imperative.

Bridging these research gaps is vital for ensuring the resilience and accuracy of ML classification systems in the dynamic IoT environment Addressing these drift issues in IoT device classification demands research efforts that span generalization, efficient drift detection, adaptive strategies, scalability, standardization, resource-efficient solutions, data-driven approaches, and robust security and privacy measures. Bridging these research gaps is essential to ensure the resilience and accuracy of ML classification systems in the dynamic IoT environment.

I. Discussion and Suggestions

In this section, we provide our discussion on addressing drift challenges in IoT device classification: (Insights and Strategies). Our comprehensive analysis of research gaps (Section 8) in IoT device classification has unearthed a series of valuable lessons that can serve as guiding principles for future endeavors in this field. These lessons encapsulate the essence of efficient drift prevention, detection, adaptation, and mitigation, as well as the broader landscape of IoT device classification.

1) Efficient Drift Prevention and Detection: The crux of maintaining the accuracy and reliability of IoT device classification models lies in the timely prevention and detection of drift. Real-time drift detection and proactive adaptation are instrumental in preserving model performance. To achieve this, researchers should explore efficient ML algorithms, such as Random Forest and LSTM, combined with strategies like algorithmic stability and online learning.

2) Standardization for Drift Adaptation: The lack of standardization in ML models and algorithms for drift handling compounds the drift issue. Establishing standardized approaches to drift detection and adaptation is vital to ensure compatibility and interoperability across different IoT setups. The adoption of ensemble methods and other standardized practices can significantly enhance the adaptability of IoT systems.

3) Model Generalization for Drift Mitigation: Drift, a recurring challenge in IoT device classification, can potentially undermine model accuracy over time. Robust model generalization stands out as a primary strategy in effectively countering drift. Therefore, researchers should explore techniques and strategies that fortify model generalization and reduce vulnerability to drift. Machine learning algorithms such as Neural Networks and SVM can help in this regard.

4) Adaptive Strategies: The dynamic nature of IoT data necessitates models that can adapt to drift without compromising their stability. Investigating and designing adaptive strategies that dynamically update models when drift is detected is crucial. Balancing the need for model stability with the necessity for adaptation becomes the cornerstone for successful implementation.

*5) Scalability Challenges***:** With the increasing deployment of IoT devices, scalability has emerged as a pressing concern. Drift introduces additional complexity, impacting accuracy and computational costs. Research must focus on scalable solutions that can accommodate the growing number of devices and the challenges posed by drift. This entails examining machine learning models such as k-means Clustering and employing IoT network metrics to assess scalability.

*6) Resource***-***Effective Solutions*: IoT devices often operate in resource-constrained environments. Drift mitigation in these settings requires resource-efficient solutions. Researchers should explore methods that minimize computational demands while effectively mitigating drift. Resource allocation algorithms and resource usage metrics can play a vital role in ensuring efficiency.

7) Data-Driven Drift Detection: IoT devices generate vast amounts of unlabeled data, complicating drift detection. Developing data-driven drift detection techniques is imperative to enhance classification accuracy. By employing data-driven detection techniques, model accuracy can be improved, even in situations where labelled training data is scarce.

8) Security and Privacy in Drift Mitigation: Security and privacy concerns remain paramount in the context of drift mitigation. Drift detection and adaptation mechanisms must be robust against potential attacks and safeguard sensitive IoT data. Employing secure machine learning models and conducting security vulnerability scans are essential components of this effort.

The multifaceted domain of IoT device classification presents unique challenges and opportunities. Our analysis has highlighted critical lessons that underscore the importance of proactive drift prevention, standardized approaches, model generalization, adaptive strategies, scalable solutions, resource-efficient methods, data-driven detection, and security measures. These lessons serve as guiding principles for researchers and practitioners in the realm of IoT device classification, ensuring that classification systems remain resilient and effective in dynamic and ever-evolving environments.

IV. Conclusion

IoT device classification is crucial for device management, security, and network management. However, drift challenges may arise, necessitating the retraining of ML models, leading to increased costs and complexity. This research paper presents a comprehensive investigation into the various aspects of machine learning techniques in the context of IoT device classification, particularly under concept of drift. The study encompasses various facts of IoT classification process, starting from prevention, detection, adaptation to mitigation. Additionally, this paper offers a comprehensive overview of the current landscape, highlighting the strengths and limitations along with future directions.

The future of drift detection in IoT device classification holds exciting potential across several key areas. First, advanced machine learning models are being developed to autonomously adapt to various types of drift, ensuring the continued accuracy of models in dynamic environments. Second, interdisciplinary collaboration is becoming increasingly crucial, with experts in ethics, law, and sociology contributing to addressing the ethical and privacy concerns surrounding drift detection. Third, edge-native drift detection models are emerging, capable of efficiently operating on IoT devices themselves, reducing the need for centralized processing. Finally, blockchain integration is being explored to enhance the security and auditability of drift detection processes.

Moreover, the future of drift management in IoT device classification, encompassing both drift adaptation and mitigation, holds immense promise. Strategies are being developed to create edge-native models and adaptation/mitigation approaches that can efficiently operate on resource-constrained IoT devices. Explainable techniques are being emphasized to ensure that adaptations and mitigation strategies remain transparent and interpretable, building trust in their functionality. Furthermore, federated learning approaches are being explored to distribute both adaptation and mitigation processes across networks of IoT devices, enabling collaborative and efficient management. These efforts also encompass ethical and privacy considerations, addressing issues like data usage, model transparency, and the responsible handling of sensitive information.

Acknowledgment

This work was supported by the Fundamental Research Grant Scheme (FRGS) of Universiti Malaysia Pahang-Al Sultan Abdullah under Grant no: FRGS/1/2023/ICT02/UMP/02/7 and RDU Grant no: RDU230144. The communication of this research is made possible through monetary assistance by Universiti Tun Hussein Onn Malaysia and the UTHM Publisher’s Office via Publication Fund E15216”.

References

[1] I. Zhou et al., "Internet of Things 2.0: Concepts, applications, and future directions," *IEEE Access*, vol. 9, pp. 70961-71012, May 2021, doi: 10.1109/access.2021.3078549.

[2] H. Mehmood et al., "Concept drift adaptation techniques in distributed environment for real-world data streams," *Smart Cities*, vol. 4, no. 1, pp. 349-371, 2021, doi: 10.3390/smartcities4010021.

[3] L. Yang et al., "CADE: Detecting and explaining concept drift samples for security applications," in *Proc. 30th USENIX Secur. Symp. (USENIX Security 21)*, 2021, pp. 2327-2344.

[4] C. Gundogan et al., "Reliable firmware updates for the information-centric internet of things," in *Proc. 8th ACM Conf. Inf.-Centric Netw.*, 2021, pp. 59-70, doi: 10.1145/3460417.3482974.

[5] H. Tahaei et al., "The rise of traffic classification in IoT networks: A survey," *J. Netw. Comput. Appl.*, vol. 154, 2020, doi:10.1016/j.jnca.2020.102538.

[6] T. S. Sethi and M. Kantardzic, "On the reliable detection of concept drift from streaming unlabeled data," *Expert Syst. Appl.*, vol. 82, pp. 77-99, 2017, doi: 10.1016/j.eswa.2017.04.008.

[7] D. M. V. Sato et al., "A survey on concept drift in process mining," *ACM Comput. Surv.*, vol. 54, no. 9, 2021, doi:10.1145/3472752.

[8] N. F. Idris and M. A. Ismail, "A review of homogenous ensemble methods on the classification of breast cancer data," *Przeglad Elektrotechniczny*, no. 1, pp. 1-10, 2024, doi: 10.15199/48.2024.01.21.

[9] N. S. Nordin and M. A. Ismail, "A hybridization of butterfly optimization algorithm and harmony search for fuzzy modelling in phishing attack detection," *Neural Comput. Appl.*, vol. 35, no. 7, pp. 5501-5512, 2023, doi: 10.1007/s00521-022-07957-0.

[10] A. Yeshchenko et al., "Comprehensive process drift detection with visual analytics," in *Proc. Int. Conf. Conceptual Model.*, 2019, pp. 119-135, doi: 10.1007/978-3-030-33223-5_11.

[11] N. L. Ab Ghani, I. A. Aziz, and M. Mehat, "Concept drift detection on unlabeled data streams: A systematic literature review," in *Proc. IEEE Conf. Big Data Anal. (ICBDA)*, 2020, pp. 61-65, doi:10.1109/icbda50157.2020.9289802.

[12] F. Bayram, B. S. Ahmed, and A. Kassler, "From concept drift to model degradation: An overview on performance-aware drift detectors," *Knowl.-Based Syst.*, vol. 245, 2022, doi:10.1016/j.knosys.2022.108632.

[13] M. Han et al., "A survey of active and passive concept drift handling methods," *Comput. Intell.*, vol. 38, no. 4, pp. 1492-1535, 2022, doi:10.1111/coin.12520.

[14] A. L. Suarez-Cetrulo, D. Quintana, and A. Cervantes, "A survey on machine learning for recurring concept drifting data streams," *Expert Syst. Appl.*, vol. 213, 2023, doi: 10.1016/j.eswa.2022.118934.

[15] F. Alwahedi et al., "Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models," *Internet Things Cyber-Phys. Syst.*, vol. 5, pp. 1-15, 2024, doi: 10.1016/j.iotcps.2023.12.003.

[16] A. Javed et al., "Machine learning and deep learning approaches in IoT," *PeerJ Comput. Sci.*, vol. 9, 2023, doi: 10.7717/peerj-cs.1204.

[17] Y. Liu et al., "Machine learning for the detection and identification of internet of things devices: A survey," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 298-320, 2021, doi: 10.1109/JIOT.2021.3099028.

[18] H. Jmila et al., "A survey of smart home IoT device classification using machine learning-based network traffic analysis," *IEEE Access*, vol. 10, pp. 97117-97141, 2022, doi: 10.1109/access.2022.3205023.

[19] N. N. M. Azam et al., "Classification of COVID-19 symptoms using multilayer perceptron," *Iraqi J. Comput. Sci. Math.*, vol. 4, no. 4, pp. 100-110, 2023, doi: 10.52866/ijcsm.2023.04.04.009.

[20] B. M. Alencar et al., "Fog-DeepStream: A new approach combining LSTM and concept drift for data stream analytics on fog computing," *Internet Things*, vol. 24, 2023, doi:10.1016/j.iot.2023.100731.

[21] A. Pesaranghader, H. L. Viktor, and E. Paquet, "McDiarmid drift detection methods for evolving data streams," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, 2018, pp. 1–9, doi: 10.1109/ijcnn.2018.8489260.

[22] B. H. Schwengber *et al.*, "A method aware of concept drift for online botnet detection," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2020, pp. 1–6, doi: 10.1109/globecom42002.2020.9347990.

[23] Q. Xiang *et al.*, "Concept drift adaptation methods under the deep learning framework: A literature review," *Appl. Sci.*, vol. 13, no. 11, p. 6515, 2023, doi: 10.3390/app13116515.

[24] G. Xie *et al.*, "A selective transfer learning method for concept drift adaptation," in *Adv. Neural Netw. (ISNN)*, vol. 10262, Springer, 2017, pp. 353–361, doi: 10.1007/978-3-319-59081-3_42.

[25] W. Li *et al.*, "DDG-DA: Data distribution generation for predictable concept drift adaptation," in *Proc. AAAI Conf. Artif. Intell.*, vol. 36, no. 4, 2022, pp. 4092–4100, doi: 10.1609/aaai.v36i4.20327.

[26] H. Yu *et al.*, "Meta-ADD: A meta-learning based pre-trained model for concept drift active detection," *Inf. Sci.*, vol. 608, pp. 996–1009, 2022, doi: 10.1016/j.ins.2022.07.022.

[27] L. Xu *et al.*, "ADTCD: An adaptive anomaly detection approach towards concept drift in IoT," *IEEE Internet Things J.*, early access, 2023, doi: 10.1109/JIOT.2023.3265964.

[28] W. Ding *et al.*, "Trend drift discovery for individual highway drivers through ensemble learning," *UMBC Faculty Collection*, 2022.

[29] D. M. Manias, A. Chouman, and A. Shami, "A model drift detection and adaptation framework for 5G core networks," in *Proc. IEEE Mediterr. Conf. Commun. Netw. (MeditCom)*, 2022, pp. 197–202, doi: 10.1109/MeditCom55741.2022.9928669.

[30] Q. Hao and Z. Rong, "IoTTFID: An incremental IoT device identification model based on traffic fingerprint," *IEEE Access*, vol. 11, pp. 58 456–58 468, 2023, doi: 10.1109/access.2023.3284542.

[31] A. Liu *et al.*, "Regional concept drift detection and density synchronized drift adaptation," in *Proc. Int. Joint Conf. Artif. Intell. (IJCAI)*, 2017, pp. 2280–2286, doi: 10.24963/ijcai.2017/317.

[32] R. S. Barros *et al.*, "RDDM: Reactive drift detection method," *Expert Syst. Appl.*, vol. 90, pp. 344–355, 2017, doi: 10.1016/j.eswa.2017.08.023.

[33] S. Marathe *et al.*, "CurrentSense: A novel approach for fault and drift detection in environmental IoT sensors," in *Proc. ACM/IEEE Int. Conf. Internet Things Design Implement. (IoTDI)*, 2021, pp. 93–105, doi: 10.1145/3450268.3453535.

[34] M. Asghari, D. Sierra-Sosa, M. Telahun, A. Kumar, and A. S. Elmaghraby, "Aggregate density-based concept drift identification for dynamic sensor data models," *Neural Comput. Appl.*, vol. 33, pp. 3267–3279, 2021, doi: 10.1007/s00521-020-05190-1.

[35] J. Lu *et al.*, "Learning under concept drift: A review," *IEEE Trans. Knowl. Data Eng.*, vol. 31, no. 12, pp. 2346–2363, Dec. 2019, doi: 10.1109/tkde.2018.2876857.

[36] X. Liu, S. H. Hussein, K. H. Ghazali, T. M. Tung, and Z. M. Yaseen, "Optimized adaptive neuro-fuzzy inference system using metaheuristic algorithms: Application of shield tunneling ground surface settlement prediction," *Complexity*, vol. 2021, doi: 10.1155/2021/6666699.

[37] F. E. Casado *et al.*, "Concept drift detection and adaptation for federated and continual learning," *Multimedia Tools Appl.*, pp. 1–23, 2022, doi: 10.1007/s11042-022-13843-7.

[38] T. Chow, U. Raza, I. Mavromatis, and A. Khan, "Flare: Detection and mitigation of concept drift for federated learning-based IoT deployments," *arXiv*, preprint arXiv:2305.08504, 2023. [Online]. Available: https://arxiv.org/abs/2305.08504.

[39] A. Antolini *et al.*, "Combined HW/SW drift and variability mitigation for PCM-based analog in-memory computing for neural network applications," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 13, no. 1, pp. 395–407, Mar. 2023, doi: 10.1109/jetcas.2023.3241750.

[40] L. Fan *et al.*, "EvoIoT: An evolutionary IoT and non-IoT classification model in open environments," *Comput. Netw.*, vol. 219, Dec. 2022, doi: 10.1016/j.comnet.2022.109450.

[41] L. Yang, D. M. Manias, and A. Shami, "PWPAE: An ensemble framework for concept drift adaptation in IoT data streams," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2021, pp. 1–6, doi: 10.1109/globecom46510.2021.9685338.

[42] R. Jordaney *et al.*, "Transcend: Detecting concept drift in malware classification models," in *Proc. 26th USENIX Secur. Symp. (USENIX Security 17)*, 2017, pp. 625–642.

[43] I. Mavromatis *et al.*, "LE3D: A lightweight ensemble framework of data drift detectors for resource-constrained devices," in *Proc. IEEE 20th Consum. Commun. Netw. Conf. (CCNC)*, 2023, pp. 611–619, doi: 10.1109/ccnc51644.2023.10060415.

[44] N. Okui, M. Nakahara, Y. Miyake, and A. Kubota, "Identification of an IoT device model in the home domain using IPFIX records," in *Proc. IEEE 46th Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, 2022, pp. 583–592, doi: 10.1109/compsac54236.2022.00104.

[45] A. Chowdhury, S. A. Raut, and H. S. Narman, "DA-DRLS: Drift adaptive deep reinforcement learning-based scheduling for IoT resource management," *J. Netw. Comput. Appl.*, vol. 138, pp. 51–65, 2019, doi: 10.1016/j.jnca.2019.04.010.

[46] Q. Chen *et al.*, "IoTID: Robust IoT device identification based on feature drift adaptation," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2021, pp. 1–6, doi: 10.1109/globecom46510.2021.9685693.

[47] C.-C. Lin, D.-J. Deng, C.-H. Kuo, and L. Chen, "Concept drift detection and adaptation in big imbalance industrial IoT data using an ensemble learning method of offline classifiers," *IEEE Access*, vol. 7, pp. 56 198–56 207, 2019, doi: 10.1109/access.2019.2912631.

[48] O. A. Wahab, "Intrusion detection in the IoT under data and concept drifts: Online deep learning approach," *IEEE Internet Things J.*, vol. 9, no. 20, pp. 19 706–19 716, Oct. 2022, doi: 10.1109/jiot.2022.3167005.

[49] L. Yang and A. Shami, "A lightweight concept drift detection and adaptation framework for IoT data streams," *IEEE Internet Things Mag.*, vol. 4, no. 2, pp. 96–101, Jun. 2021, doi: 10.1109/iotm.0001.2100012.

[50] F. Bayram *et al.*, "DA-LSTM: A dynamic drift-adaptive learning framework for interval load forecasting with LSTM networks," *Eng. Appl. Artif. Intell.*, vol. 123, Aug. 2023, doi: 10.1016/j.engappai.2023.106480.

[51] B. Bayram, B. Köroğlu, and M. Gönen, "Improving fraud detection and concept drift adaptation in credit card transactions using incremental gradient boosting trees," in *Proc. 19th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, 2020, pp. 545–550, doi: 10.1109/icmla51294.2020.00091.

[52] M. Jain, G. Kaur, and V. Saxena, "A K-means clustering and SVM based hybrid concept drift detection technique for network anomaly detection," *Expert Syst. Appl.*, vol. 193, May 2022, doi: 10.1016/j.eswa.2022.116510.

[53] M. Stallmann, A. Wilbik, and G. Weiss, "Towards unsupervised sudden data drift detection in federated learning with fuzzy clustering," in *Proc. IEEE Int. Conf. Fuzzy Syst. (FUZZ-IEEE),* 2024, pp. 1-8, doi:10.1109/fuzz-ieee60900.2024.10611883.

[54] S. Dong, Q. Wang, S. Sahri, T. Palpanas, and D. Srivastava, "Efficiently mitigating the impact of data drift on machine learning pipelines," *Proc. VLDB Endow.*, vol. 17, no. 11, pp. 3072-3081, Jul. 2024, doi: 10.14778/3681954.3681984.