Drift Detection and Model Update using Unsupervised AutoML in IoT

MOHAMED KHALAFALLA HASSAN[1,2,3], IBRAHIM YOUSIF ALSHAREEF[2]
[1]University Technology Malaysia,
MALAYSIA

[2]Faculty of Telecommunication Engineering,
Future University,
SUDAN

[3]Faculty of Engineering,
University De Moncton,
CANADA

Abstract: - This paper addresses the challenges of concept drift on the Internet of Things (IoT) environments and evaluates a machine-learning model's performance under varying data drift conditions using unsupervised Automatic Machine Learning (AutoML) anomaly detection techniques. By implementing a dynamic learning framework and employing advanced analytics, the study showcases the resilience of the proposed methodology against evolving data patterns. The results demonstrate the model's robust predictive capabilities, even in high drift scenarios, underscoring the importance of adaptive models in maintaining effective IoT security measures. The achieved improvement percentages can reach 46% for the F1 score.

Key-Words: - Feature drift, AutoML, unsupervised learning, Anomaly detection, IoT, Cybersecurity

Received: August 18, 2023. Revised: November 12, 2023. Accepted: December 7, 2023. Published: December 31, 2023.

1 Introduction

In recent years, there has been a significant surge in the use of Internet-based networks, especially the Internet of Things (IoT) and Wireless Sensor Networks (WSN), [1]. These technologies have profoundly transformed various sectors, including healthcare [2], transportation [3], education [4] and aviation [5]. The last decade has seen a dramatic rise in the integration of IoT across societal facets, [1]. Since 2018, the global investment in IoT has consistently grown, surpassing $40 billion, with forecasts indicating it might exceed $1.1 trillion by 2024, [6]. Concurrently, IoT devices have expanded, enhancing innovative management and telemetry. This boom has accelerated digitalization, allowing physical objects to interact with the internet and turning networks into data-rich sources. However, this widespread connectivity poses considerable cyber threats, highlighting the need for robust security measures, [7].

During this era, certain traffic types diminished due to widespread COVID-19 lockdowns and the shift towards remote working. This change highlighted the necessity for predictive frameworks in cybersecurity to be adaptable and responsive to evolving traffic patterns, maintaining their effectiveness and relevance, [8], [9]. The early identification of concept drift is crucial for the accuracy of online and offline classifiers. Existing point detectors show limitations in detecting concept drift, emphasizing the need for more sophisticated detectors. These should be capable of monitoring multivariate data streams and identifying shifts in their correlation with the label class, thereby preserving the integrity of classification systems in dynamic settings, [7], [10]. The realm of detection, also known as dynamic learning or anomaly detection, encompasses a variety of detectors that evolve and are applicable in mathematical modelling and machine learning (ML), [8], [9], [11], [12], [13]. Two primary methods determine concept drift in streaming data: ML and statistical techniques, [14]. The ML approach adjusts model characteristics in an online or incremental manner, [15] or uses ensemble classifiers trained on different stream segments to optimize detection, [16]. While classifier retraining is feasible, many models lack explicit drift detection mechanisms. The ML strategy, focused on error metric changes, aims to

sustain classifier performance amidst data shifts. A pivotal element is the accurate detection of concept drift occurrence. An alert system, which triggers at drift onset and remains until its identification, is crucial, particularly in network monitoring and malware detection, where prompt drift response boosts system resilience and effectiveness, [16].

The traditional statistical approach focuses on tracking error statistics and mistake rates based on statistical learning theory principles. The statistical change point detection algorithm, which identifies significant shifts in data's statistical properties through statistical testing, is widely used in this context. Another method involves a sliding window technique, where the model is trained on recent data in a fixed-size window, shifting forward as new data comes in, allowing adaptation to data distribution changes, [7].

The paper's objective is to create and implement a dynamic learning framework. This framework will incorporate incremental anomaly detection, using methods like the unsupervised ML and Friedman statistical tests, and blend it with AutoML using Pycaret, [17], for ongoing model selection and updates. This strategy will boost the IDS's adaptability and responsiveness to changing data patterns and new threats. Finally, we will apply this dynamic learning framework to the latest and most comprehensive IoT dataset. Using the framework for contemporary data ensures its relevance and effectiveness in the current IoT security context. This step is vital for proving the proposed methods' real-world viability, providing the IDS can effectively counter existing and emerging security threats in the IoT sphere. This paper is organized as follows: the next section will highlight the most notable related work, followed by the methodology starting with the overall flowchart, dynamic learning, and the dataset, then we will go through the results and discussion, and finally, a conclusion.

2 Related Works

The literature covered in this section will mainly highlight the efforts that addressed concept and feature drifts and model updates. In their study, researchers in [18], recommended integrating a Deep Belief Network (DBN) with intrusion detection systems for IoT networks. This DBN method focuses on detecting ongoing irregularities within the IoT network, offering a higher detection probability than other methods. Another team in [19], developed a hierarchical intrusion detection model, the Stacked De-noising Auto-encoder Support Vector Machine (SDAE-SVM). This model is based on a three-layer neural network and aims to assess the effectiveness of a deep learning de-noising auto-encoder in bolstering IoT security. It employs a layer-by-layer pretraining and fine-tuning method to minimize dimensionality, achieving an impressive accuracy rate of 98%, though no updates to the model were provided. In [20], researchers presented an intelligent intrusion detection system (IIDS) tailored for IoT environments. This study explored the feasibility of using ML algorithms for IDS in resource limited IoT networks. An advanced IDS, combining network virtualization with Deep Learning (DL) algorithms, was developed to detect anomalies in IoT networks. The system's effectiveness was evaluated against five types of attacks, including blackhole, opportunistic service, DDoS, sinkhole, and wormhole attacks. Results showed an average precision rate of 95% and a recall rate of 97% across these scenarios, as determined by analysing precision-recall curves. Another study, [21] introduced online ML to tackle concept drift in IDS. The proposed method utilized an interleaved-test-then-train approach, where the ML model is continuously tested and trained with each new data block. Implementing several unsupervised learning algorithms led to accuracies up to 99.56%. However, the study did not use an IoT-specific dataset, a crucial element for ensuring the solution's real-world applicability and relevance in the IoT context. In [22], the authors introduced 'ElStream,' a cutting-edge framework combining ensemble and traditional ML techniques for concept drift detection. ElStream distinguishes itself through its majority voting mechanism, selectively employing the most effective classifiers for decision-making. ElStream's ensemble learning component consistently demonstrated strong performance when applied to real and artificial datasets. Its superiority was evident in accuracy improvements over previous benchmarks and conventional ML methods. ElStream achieved accuracy enhancements of 12.49% on the PokerHand dataset, 11.98% for LED, 10.06% for Random RBF, 1.2% for electricity, and 0.33% for SEA. These results highlight ElStream's potential as a significant leap forward in concept drift detection, offering marked improvements over existing approaches. Many current frameworks utilize online ML techniques for drift detection. However, these methods typically require significant computational resources and extensive hyperparameter optimization. In addition, no study has yet explored the use of AutoML frameworks in this context. AutoML has the

potential to revolutionize this field by automating the selection of the best algorithms and optimizing hyperparameters, thereby enhancing the effectiveness and efficiency of attack detection and classification in IDS for IoT.

3 Methodology

The following section will discuss the methodological aspects of the proposed research. Figure 1 shows the overall flowchart.

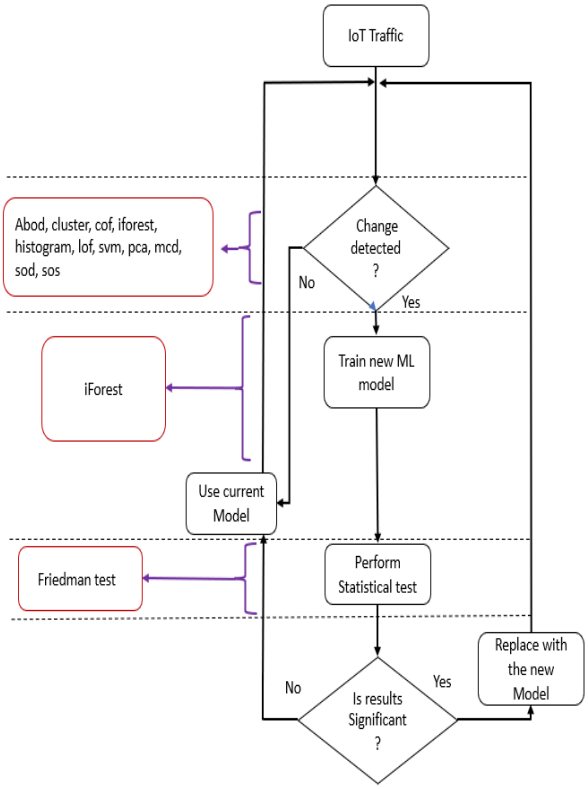

Fig. 1: Overall flowchart

The flowchart represents a decision-making process for updating ML models based on detecting concept drift in Internet of Things (IoT) traffic. Initially, IoT traffic is monitored for changes. If a change is detected, training a new ML model is initiated. Various anomaly detection algorithms, such as Angle-Based Outlier Detection (ABOD), clustering, Connectivity-Based Outlier Factor (COF), Isolation Forest (iForest), histogram-based outlier detection, Local Outlier Factor (LOF), Support Vector Machine (SVM), Principal Component Analysis (PCA), Minimum Covariance Determinant (MCD), Subspace Outlier Detection (SOD), and Stochastic Outlier Selection (SOS), are considered, the feature drift is identified based on calculated anomaly score for each features, if the majority algorithms identify the feature as anomaly, then it will be marked as a drifted feature if it is greater than a predefined threshold, the AutoML is used to streamline the selection of an optimum model and fine-tune the hyperparameters to accommodate the new data distribution, thus maintaining model performance. If no change is detected, the current model continues to be used. In parallel, a statistical test, specifically the Friedman test, is employed to validate the significance of the results from the new model. If the results are not significant, the current model remains in use. If the results are significant, the system replaces the current model with the new, updated model. This framework ensures that the IDS remains effective by adapting to the evolving data patterns characteristic of IoT environments.

ALGORITHM 1 DYNAMIC LEARNING

input: f_{IoT_i}: *Feature i in IoT dataset* X_{IoT}, *i: index, j: index, u: index,* $K'[]$: *Anomaly algorithms,* Ω': *count of anomaly detected,* δ_{u-1}: *old model.*
Output: $W_{j_{IoT}}$: *window,* δ_u: *Statistically significant ML mode*
01: begin
02: *for all* $f_{IoT_i} \in X_{IoT}$ **do**
subscriptionssubscriptions03: $W_{j_{IoT}} \leftarrow W_{j_{IoT}} \cup [f_{IoT_i}]$; // *provided* f_{IoT_i} *is not redundant.*
04: for all Anomaly algorithms in $K'[]$ **do**
05: $\Omega' \leftarrow$ *find for each* f_{IoT_i} *count of anomaly detected*
06: **If** $\Omega' >$ *than threshold // by majority then*
07: *Stop forecasting at* $W_{j_{IoT}}$ *// change is detected*
08: $\delta_u \leftarrow$ *train new random forest*
09 **If** δ_u *is significantly better than* δ_{u-1} **then** // *Friedman.*
10: *replace* δ_{u-1} *by* δ **else if**
11: *keep* δ_u
12: *endif*
13: endif
14: Loop

3.1 Dataset

This paper highlights the integration of the CICIoT2023 dataset, [1], an updated IoT data repository developed by the Canadian Institute of Cybersecurity. Existing datasets often fall short, offering a limited array of attack simulations and not using genuine IoT devices to mirror complex network topologies. The CICIoT2023 dataset addresses this by featuring 33 unique attacks across a network of 105 IoT devices, categorized into seven types: DDoS, DoS, Reconnaissance, Web-based, Brute Force, Spoofing, and Mirai. All attacks are conducted by and directed at IoT devices, thus providing authentic scenarios for security analysis. Unlike other datasets, CICIoT2023 enriches IoT security resources with new attacks like ACK Fragmentation, Slow Loris, UDP Fragmentation, Command Injection, and Browser Hijacking, [1]. It offers a diversity of data formats, meeting varied research needs and detailing attack types, characteristics, definitions, and statistics—detailed

information on network topology and device specifications is available in [1].

When citing references in the text of the abstract, type the corresponding number in square brackets as shown at the end of this sentence [1].

4 Results and Discussions

Table 1 shows the final output of the retraining for the drifted features, representing the final output of Algorithm 1.

Table 1. Algorithm1 Results

Feature	**Random Forest 25% Drift**			
IAT	***Accuracy***	***Recall***	***Precision***	***F1 score***
	0.9916	0.9916	0.9912	0.9910
	Random Forest 50% Drift			
	0.9723	0.9723	0.9700	0.9711
	Random Forest 100% Drift			
	0.9122	0.9122	0.9110	0.9115

The Table 1 presents a performance evaluation of a Random Forest classifier under varying degrees of concept drift, using the Inter-Arrival Time (IAT) feature for classification. Three scenarios correspond to the data's 25%, 50%, and 100% drift. In the first scenario, with 25% drift, the Random Forest classifier maintains an impressive performance with accuracy and recall of 0.9916, precision of 0.9912, and an F1 score of 0.9910. This indicates a high consistency between precision and recall, reflecting the model's balanced capability in class identification. As the drift increases to 50%, all metrics show a slight decrease, with accuracy, recall, and F1 score at 0.9723 and precision at 0.9700. This suggests that the classifier is still robust but begins to experience a dip in performance due to the increased variability in the data. At 100% drift, the performance further declines, yet the classifier remains relatively strong with accuracy and recall of 0.9122, precision of 0.9110, and an F1 score of 0.9115. Even with complete drift, the model exhibits substantial resilience, although the decrease in metrics indicates more pronounced effects of concept drift. These findings illustrate that while the Random Forest algorithm is generally robust to concept drift, its performance does degrade as the drift increases. However, the degradation is not proportional to the increase in drift, showcasing the model's effectiveness in adapting to changes in data patterns. This performance assessment is crucial for practitioners and researchers in predictive modelling, particularly in dynamic environments where concept drift is a concern.

Figure 2 shows the improvement percentages to our benchmark in [1].

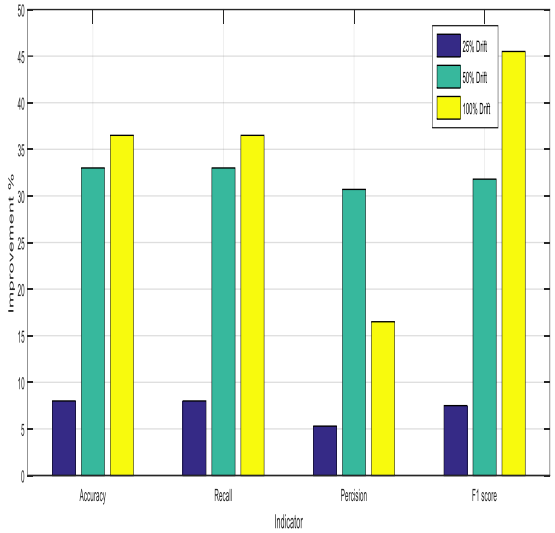

Fig. 2: Improvement percentages

Figure 2 shows that the improvement percentages increased compared to the benchmark in [1], for 25%, 50%, and 100%, respectively, where the highest improvement was recorded for the F1 score in the 100% drift, which suggests that the proposed methodology can be efficient even in highly drifted features which eventually will improve the models' reliability and validity.

5 Conclusion

In conclusion, this paper has successfully addressed the challenge of concept drift in IoT environments by implementing a dynamic learning framework validated using the comprehensive CICIoT2023 dataset. The framework's adaptability was rigorously evaluated across various drift scenarios, demonstrating its robustness and effectiveness. Results indicate that while performance metrics slightly decline with increased drift, the resilience of the model's predictive capabilities is evident using the proposed methodology. The contribution of this research is pivotal, offering significant advancements in the development of reliable security analytics for the ever-evolving IoT domain, ensuring that IDS systems remain effective against a wide array of sophisticated attacks.

References:

[1] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment", *Sensors* 2023, 23, 5941. https://doi.org/10.3390/s23135941.

[2] S. Selvaraj and S. Sundaravaradhan, "Challenges and opportunities in IoT healthcare systems: a systematic review," *SN Applied Sciences,* vol. 2, no. 1, p. 139, 2020.

[3] F. Zantalis, G. Koulouras, S. Karabetsos, and D. Kandris, "A review of machine learning and IoT in smart transportation," *Future Internet,* vol. 11, no. 4, p. 94, 2019.

[4] M. Al-Emran, S. I. Malik, and M. N. Al-Kabi, "A survey of Internet of Things (IoT) in education: Opportunities and challenges," *Toward social internet of things (SIoT): Enabling technologies, architectures and applications: Emerging technologies for connected and smart social objects,* pp. 197-209, 2020.

[5] J. Pate and T. Adegbija, "AMELIA: An application of the Internet of Things for aviation safety," in *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 2018: IEEE, pp. 1-6.

[6] M. Amin, F. Al-Obeidat, A. Tubaishat, B. Shah, S. Anwar, and T. A. Tanveer, "Cyber security and beyond: Detecting malware and concept drift in AI-based sensor data streams using statistical techniques," *Computers and Electrical Engineering,* vol. 108, p. 108702, 2023.

[7] R. K. Z. S. M. S. Noori, A. Sali and F. Hashim, "Feature Drift Aware for Intrusion Detection System Using Developed Variable Length Particle Swarm Optimization in Data Stream," *IEEE ACCESS,* vol. 11, pp. 128596-128617,2023, doi: 10.1109/ACCESS.2023.3333000.

[8] M. K. Hassan *et al.*, "DLVisor: Dynamic Learning Hypervisor for Software Defined Network," *IEEE Access,* 2023.

[9] M.K. Hassan *et al.*, "Dynamic learning framework for smooth-aided machine-learning-based backbone traffic forecasts," *Sensors,* vol. 22, no. 9, p. 3592, 2022.

[10] L. Yang and A. Shami, "A lightweight concept drift detection and adaptation framework for IoT data streams," *IEEE Internet of Things Magazine,* vol. 4, no. 2, pp. 96-101, 2021.

[11] D. Kim, Y.-H. Han, and J. Jeong, "Design and Implementation of Real-time Anomaly Detection System based on YOLOv4," *WSEAS Transactions on Electronics,* vol. 13, pp. 130-136, 2022, https://doi.org/10.37394/232017.2022.13.17.

[13] D. Lee, H. Choo, and J. Jeong, "Anomaly Detection based on 1D-CNN-LSTM Auto-Encoder for Bearing Data," *WSEAS Transactions on Information Science and Applications,* vol. 20, pp. 1-6, 2023, https://doi.org/10.37394/23209.2023.20.1.

[13] N. Baci, K. Vukatana, and M. Baci, "Machine learning approach for intrusion detection systems as a cyber security strategy for Small and Medium Enterprises," *WSEAS Transactions on Business and Economics,* vol. 19, pp. 474-480, 2022, https://doi.org/10.37394/23207.2022.19.43.

[14] B. Pishgoo, A. A. Azirani, and B. Raahemi, "A dynamic feature selection and intelligent model serving for hybrid batch-stream processing," *Knowledge-Based Systems,* vol. 256, p. 109749, 2022.

[15] J. P. Barddal, H. M. Gomes, F. Enembreck, and B. Pfahringer, "A survey on feature drift adaptation: Definition, benchmark, challenges and future directions," *Journal of Systems and Software,* vol. 127, pp. 278-294, 2017.

[16] S. Sahmoud and H. R. Topcuoglu, "A general framework based on dynamic multi-objective evolutionary algorithms for handling feature drifts on data streams," *Future Generation Computer Systems,* vol. 102, pp. 42-52, 2020.

[17] M. Ali, "PyCaret: An open source, low-code machine learning library in Python," *PyCaret version,* vol. 2, 2020.

[18] N. Balakrishnan, A. Rajendran, D. Pelusi, and V. Ponnusamy, "Deep Belief Network enhanced intrusion detection system to prevent security breach in the Internet of Things," *Internet of things,* vol. 14, p. 100112, 2021.

[19] Z. Lv, L. Qiao, J. Li, and H. Song, "Deep-learning-enabled security issues in the internet of things," *IEEE Internet of Things Journal,* vol. 8, no. 12, pp. 9531-9538, 2020.

[20] G. Thamilarasu and S. Chawla, "Towards deep-learning-driven intrusion detection for the internet of things," *Sensors,* vol. 19, no. 9, p. 1977, 2019.

[21] C. Nixon, M. Sedky, and M. Hassan, "Practical application of machine learning

based online intrusion detection to internet of things networks," in *2019 IEEE Global Conference on Internet of Things (GCIoT)*, 2019: IEEE, pp. 1-5.

[22] A. Abbasi, A. R. Javed, C. Chakraborty, J. Nebhen, W. Zehra, and Z. Jalil, "ElStream: An ensemble learning approach for concept drift detection in dynamic social big data stream learning," *IEEE Access,* vol. 9, pp. 66408-66419, 2021.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

Mohamed Khalafalla Hassan carried out the simulation, and the optimization and Manuscript writing. Ebrahim Yousif Elsharief caried out manuscript validation and verification

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare.