https://doi.org/10.7840/kics.2024.49.2.321

AI Model Stability in Industrial IoT Intrusion Detection: Leveraging the Characteristics Stability Index

Love Allen Chijioke Ahakonye◆, Cosmas Ifeanyi Nwakanma*, Jae Min Lee*, Dong-Seong Kim°

ABSTRACT

In Industrial Internet of Things (IIoT) environments, the reliability and adaptability of machine learning models are crucial for accurate decision-making. This paper introduces the Characteristic Stability Index (CSI) to monitor and ensure the stability of models in the context of heterogeneous IIoT sensor data. The CSI quantifies the variations in feature importance rankings, enabling the early detection of data drift and shifts. The experimentation results validate the performance of the decision tree algorithm to provide actionable insights, facilitating domain experts' adaptability and enhancing decision-making while minimizing operational risks and costs in the choice of intrusion detection systems model.

Key Words : AI, Characteristic Stability Index, Datasets, Deep learning, IIoT, Machine Learning

Ⅰ. Introduction

Disruptive technologies like the Internet of Things (IoT) and artificial intelligence (AI) are reshaping industries and daily life, including complex industrial domains[1,2]. The impact of IoT has extended to critical industry processes, ushering in the industrial Internet of Things (IIoT), fostering intelligent data acquisition and informed decision-making[1,2]. Similarly, AI's reach is extensive, spanning industrial operations and encompassing automatic anomaly detection[3-7].

As industries evolve, efficient AI-based intrusion detection systems (IDS) gain significance[4,8,9]. While existing IDS methods handle intrusions and attacks well[10], the expanding industrial Internet of Things (IIoT), with its diverse heterogeneous sensor data, larger attack surface, and evolving security challenges, emphasizes stable IDS algorithms[11,12]. The complex, varied IIoT sensor data poses challenges like varying granularity, multiple formats, spatial distribution, and interdependence, requiring robust algorithms for consistent detection and classification[13,14]. Combining stable IDS algorithm with transformative IoT and AI potential promises a more secure industrial landscape[15].

In the contemporary cybersecurity landscape, intrusion detection has witnessed a remarkable surge in the application of machine learning (ML) techniques[5,8,14]. Amid the evaluation of model performance across different ML methods and dataset attributes, it is crucial to recognize the pivotal role of model stability in achieving dependable and credible predictions[10]. Effectively quantifying the stability of a model through a stability index assessment gauges the consistency and alignment of

※ This work was supported by Priority Research Centers Program through the NRF funded by the MEST(2018R1A6A1A03024003 (34%)) and by the MSIT, Korea, under the Innovative Human Resource Development for Local Intellectualization support program (IITP-2024-2020-0-01612 (33%)) supervised by the IITP, and by NRF-2022R1I1A3071844 (33%).
◆ First Author : Kumoh National Institute of Technology, Department of IT Convergence Engineering, loveahakonye.ac.kr, 학생회원
° Corresponding Author : Kumoh National Institute of Technology, Department of IT Convergence Engineering, dskim@kumoh.ac.kr, 종신회원
* Kumoh National Institute of Technology, Department of IT Convergence Engineering
논문번호 : 202310-088-0-SE, Received August 30, 2023; Revised Novemver 15, 2023; Accepted Novemver 21, 2023

feature importance rankings across independent training iterations[13,16]. It is crucial for countering covariate shifts, which arise from evolving statistical attributes of input data[16-19]. Inadequate stability in feature importance can hinder the extraction of meaningful insights and lead to precarious interpretations of the model's behavior[17,20]. Consequently, the stability index becomes a cornerstone in data analysis and modeling, particularly within the context of ML[16,20].

Ensuring consistent performance mandates the evaluation of ML model stability[16-18,21-24], due to the continuous evolving intrusion and attack mechanisms in IIoT. Traditional variable selection techniques face challenges in the intricate and noisy landscape of the IIoT data, such as being time-intensive and rigid in parameterization, rendering them inappropriate[20]. The Characteristics Stability Index (CSI) is a valuable metric for appraising ML model stability. It measures the consistency and dependability of feature importance rankings across multiple training iterations, offering insights into the model's performance reliability and predictive accuracy. It is handy for evaluating how changes in data distributions or other variations influence model stability[18-20].

The paper's structure unfolds as thus: Section I. establishes context, and Section II. discusses related works on the probability and characteristics stability index metrics for monitoring model performance. Section III . delineates the system model, while Sections IV . and V . expound on outcomes and conclusions

Specifically, this study focuses on the following:

1. Assessment of the CSI stability of some stateof-the-art ML models to show the consistency and reliability of the feature importance rankings across different compared datasets.
2. Comparison of the CSI stability of varying ML models to determine which model exhibits more consistent behavior and is better suited for generating dependable predictions.
3. To verify the importance of features significant to the model predictions by examining the consistency of the relative importance of features across evaluated datasets.
4. To provide valuable, informed decision-making with the stability insights provided by CSI to aid researchers, domain experts, and stakeholders in making choices about model deployment and use based on its stability characteristics.

Ⅱ. Related Works

This research represents an extended iteration of the paper "Verifying the Stability of Tree Algorithms on Complex Industrial Internet of Things Dataset," authored by the same scholars presented at the Korean Telecommunications Society Summer Conference 2023[13]. To build on earlier research, the current study explores the body of literature on the subject, adding new scenarios and algorithms to increase the potential applicability of the suggested methodology.

A research study compared the population stability index (PSI) and the population accuracy index (PAI) through seventy-eight deliberate adjustments in the distribution of three explanatory variables within a theoretical predictive model[18]. This exploration examined categorical variable distributions and the impact of variable discretization on stability assessment, comparing PSI and PAI in two scenarios. The findings highlighted the collaborative nature of these indicators, compensating for each other's limitations in assessing variable distribution stability within the model.

Authors[24] outline PSI's limitations and introduce the PAI as an improved alternative in the banking sector, where models developed on historical data are applied to loans, ensuring a model's relevance to new data is vital. The study highlights PAI's enhanced qualities and interpretation, asserting that it accurately represents population stability. It can aid risk analysts and managers in gauging the ongoing suitability of the model.

Illustrating the application of bootstrapping to assess prediction model stability during development, authors[25] introduced diverse visualizations and metrics to effectively quantify instability, aiming for their seamless integration into routine presentations by model developers. Emphasizing the postdevelopment

monitoring of model stability, they recommended incorporating instability plots and metrics in communication with stakeholders, particularly healthcare professionals and patients. These tools aid in evaluating the model's reliability for new subjects and facilitate systematic reviews and peer assessments for comprehensive model evaluation.

To address the need for quantitative assurance of model reliability, research focuses on investigating the stability of ML approaches, particularly significant in IIoT applications enhancing our comprehensions, such as monitoring systems for anomaly, intrusions, and attack detection[13,15,20,21,26,27]. This importance becomes evident in scenarios requiring conclusive intrusion and attack identification.

Ⅲ. System Methodology

3.1 Model Stability Concerns

Model stability, a comprehensive concept impacting systems analysis, modeling, and control, spans various domains, encompassing diverse algorithms[13,16,17,20,21], notably complex dynamical networks. Initially introduced within the context of variable selection[20], stability characterizes the sensitivity of algorithms to training dataset changes, which, if overlooked, can lead to erroneous inferences and unreliable model design[28]. Various studies[26] underscore that even the same algorithm can yield different variable subsets with varying training sets.

Contrary to the CSI, the typical model validation metric, the population stability index (PSI) quantifies distribution changes in a variable over time or between two samples and enables tracking shifts in population characteristics, aiding in detecting possible model performance issues[16,19,24,25,29]. CSI gauges the algorithm's performance sustainability over time with varying data distributions, specifically examining feature importance rankings, ensuring the model can deliver dependable predictions amid changing conditions. It validates the model's efficacy by quantifying the constancy of vital features across diverse scenarios.

3.2 Characteristics Stability Index Model

In this study, the CSI assessed the stability of three representative predictive ML models for IIoT intrusion detection, focusing on data feature importance rankings. It measured the consistency of these rankings across different training iterations and dataset variations, ensuring robust relationships between features and outcomes. Moreover, it quantified feature stability amidst changing data, which is vital for reliable predictions in real-world scenarios. It offers quantifiable insights into model reliability over time and evolving data distributions, which is essential for practical applications. Fig. 1 is the pipeline flow of the CSI model.

The CSI evaluated the stability of representative ML intrusion detection algorithms using a numerical index to measure consistency across various data scenarios. Its standardized approach ensures a consistent evaluation process, avoiding subjective assessments and providing a clear benchmark for comparing algorithms. The CSI's ability to introduce

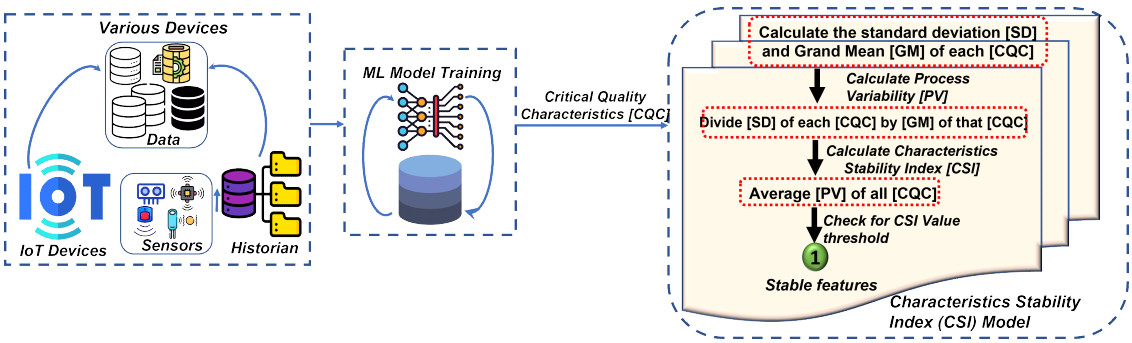


Fig. 1. Pipeline of the Characteristics Stability Index (CSI) for verifying the stability of data features for Intrusion Detection using Tree Algorithms

controlled perturbations and measure their impact identifies vulnerabilities, aiding in fine-tuning algorithms and improving stability. The feedback provided by the CSI is essential in making ML intrusion detection algorithms more reliable and resilient in real-world applications. The index provided by the CSI assesses and compares the stability of various intrusion detection approaches, contributing to selecting the most robust solutions. The CSI process includes documentation, enhancing reproducibility, and contributing to transparency and reliability. Decision-makers can use the CSI index to understand the algorithm's reliability and make informed choices based on stability considerations. The CSI process is essential in providing a comprehensive stability assessment, ensuring more informed decision-making in deploying ML-based intrusion detection.

The systematic approach to the CSI process model assesses the stability of ML algorithms to ensure that the IIoT IDS models are robust and dependable across different training iterations and dataset variations. While the exact CSI calculation approach may vary depending on the specifics of the model and dataset, below is the pipeline for the CSI calculation:

1. Initial model training and feature importance calculation: Here, the ML model trains on the original dataset, then calculates each feature's importance scores using a suitable method of choice.
2. Generate variations: Variations of the training dataset are created by perturbing data points to stimulate variations in the data distribution.
3. Recalculate feature importance: Each variation of the training dataset retrains the same model and calculates each feature's importance scores.
4. CSI calculation: The original model's feature importance scores are compared and measured with the variations' scores. The standard deviation measured the difference between the importance scores.
5. CSI value aggregating: Calculating the average of the differences by aggregating the differences calculated in the previous step across all variations gives the CSI value.
6. Setting threshold: Considering the intrusion and attack detection issue in IIoT, a CSI threshold value of 1 is determined to evaluate the stability of the process, specifically for anomaly detection purposes. where 1 represents stable.
7. CSI interpretation: Compare the calculated CSI value for each feature against the predefined threshold of 1. A CSI value of 1 indicates that the feature's importance rankings are stable across variations and iterations, highlighting the stability of the feature's importance rankings and suggesting the sensitivity of the model's performance to changes in the data distribution.
8. Application of findings: The CSI values assess the stability of the models' feature importance rankings, and the result enables informed decisions about the reliability and robustness of the model predictions under various conditions.

It is worth highlighting that the formulation and computations of the CSI can exhibit variability, contingent upon the method opted for gauging disparities in feature importance rankings. Furthermore, determining the appropriate threshold for acceptable CSI values should be informed by domain expertise and the particular demands of the application. Algorithm 1 summarizes the process of the CSI approach.

Algorithm 1. Characteristics Stability Index (CSI)

```
Train model on the original dataset
Calculate feature importance scores
Create variations of the training dataset
for each variation do
    Retrain model with variation
    Calculate feature importance scores for variation
end for
for each feature do
    Calculate importance score differences
    Use distance metric to quantify differences
end for
for each feature do
```

13: Calculate CSI value by aggregating differences
14: end for
15: Determine stability threshold
16: for each feature do
17: if CSI value ≤ threshold then
18: Feature importance rankings are stable
19: else
20: Feature importance rankings are not stable
21: end if
22: end for
23: Use CSI values for model assessment

3.3 Characteristics Stability Index Analysis

To ascertain the CSI of IIoT data, information regarding the model's critical quality characteristics (CQCs) is collected to facilitate the computation of the CSI. This index is employed to gauge the stability of the decision tree model. The acquired data enables the determination of the grand mean (GM) and standard deviation (SD) for each CQC. Aggregating the process variability (PV) across all CQCs, with PV calculated as the ratio of SD to GM for each CQC computes the CSI. Comparing the calculated CSI against a predefined threshold of 1 assesses the model stability for anomaly detection. This evaluation aids in understanding the strength and robustness of the ML process for identifying anomalies. Equation 1 establishes the characteristic stability index.

$$CSI = \frac{1}{N}\sum_{i=1}^{N}\frac{|F_i^{(O)} - F_i^{(V)}|}{\max(F_i^{(O)}, F_i^{(V)})} \leqslant \text{Threshold}, \quad (1)$$

where N represents the number of data features, $F_i^{(O)}$ is the feature importance score of the *ith* feature in the original model and $F_i^{(V)}$ gives the feature importance score of the *ith* feature in a variation of the model.

CSI thresholds are context-dependent and rely on factors like the application and data attributes. Selecting an appropriate CSI threshold entails factoring in domain expertise, analysis objectives, and data traits[23]. This research employed a point of 1 to denote the stability threshold, demonstrating the model's significance in precise predictions throughout variations and iterations.

Ⅳ. Performance Evaluation

4.1 Dataset Description and Experimental Environment

This study leverages the WUSTL_2018[30][1] and WUSTL-IIoT-2021[5][2]: datasets for the attack traffic, comprising IIoT network data for cybersecurity research. The dataset includes various IoT attacks, such as distributed denial of service, command injection, backdoors, and reconnaissance. The WUSTLIIoT-2021 dataset size is approximately 2.7 GB and covers about 53 hours of data samples. It was generated using the IIoT testbed[5], designed to closely mimic real-world industrial systems and enable the execution of authentic cyber-attacks. The model experimentation was with total data observations of the 1,194,464, 1,107,448 normal samples, 87,016 attack samples, and 41 data features split using the train-test-split modules in Keras and Scikit-learn in the proportion of training (60%), testing (25%), and validation (15%), respectively, for reproducibility. The dataset was selected based on its relevance to cyberattacks in IIoT networks. Table 1 shows the dataset attack descriptions.

The simulation environment is a system equipped with an Intel Core i5-8500 CPU @ 3.00GHz and 8GB

Table 1. Statistical Details of the Evaluated WUSTL-IIoT-2021 and WUSTL-2018 Datasets

Dataset	Traffic	Percentage (%)
WUSTL -IIoT-2021	Normal Traffic	92.72
	Command Injection Traffic	0.023
	DoS Traffic	6.55
	Reconnaissance Traffic	0.69
	Backdoor Traffic	0.017
	Total	100
WUSTL -2018	Normal Traffic	93.93
	All Attacks	6.07
	Total	100

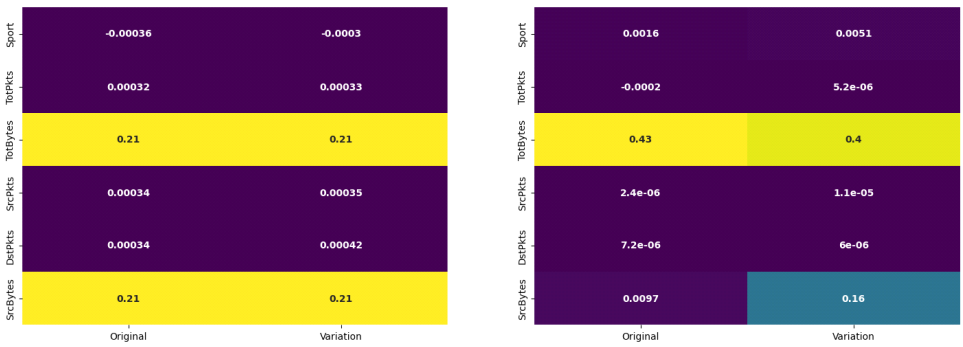
1) https://www.cse.wustl.edu/jain/iiot/index.html
2) https://ieee-dataport.org/documents/wustl-iiot-2021

RAM, using Python 3.0. This study evaluated the Decision Tree, Random Forest, Naive Bayes, and Deep Neural Network (DNN) due to their significance and dominance in classification problems. Moreover, it established notable performance in processing large, complex, and noisy data[10,21]. The choice of the four (4) representative algorithms hinges on their established performance[8,10,15].

4.2 Summary of Evaluation

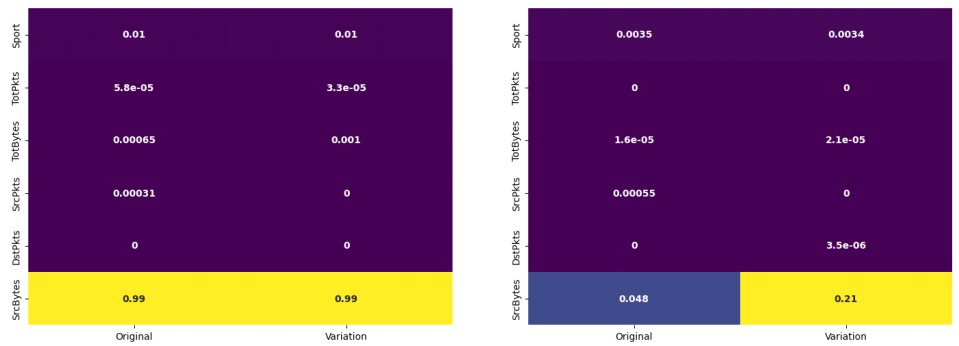
Fig. 2 is a heatmap visually comparing the feature importance rankings between the original and the variation of the decision tree and random forest models in binary classification. A side-by-side comparison of the degree of feature importance rankings between the original and the varied model with the purple color representing the higher distribution. Similarly, is provided in Fig. 3 measuring the feature importance rankings of the naive bayes and deep neural networks. It distinguishes the degree of the feature importance rankings by the evaluated variant and original models. Notably, a high degree of variability represented in yellow shows the instability of the naive bayes and DNN in IIoT data. Each feature shows how its importance value differs between the initial and variation scenarios. The higher importance value indicates that the feature substantially influences the model's predictions. Comparing these values in the heatmap enables insights into how changes in the model or data affect the relative importance of features.

Analyzing the feature rankings of the evaluated models in CSI performance in a multi-class scenario, Fig. 4 and Fig. 5 illustrate the degree of stability by the decision tree, random forest, naive bayes, and



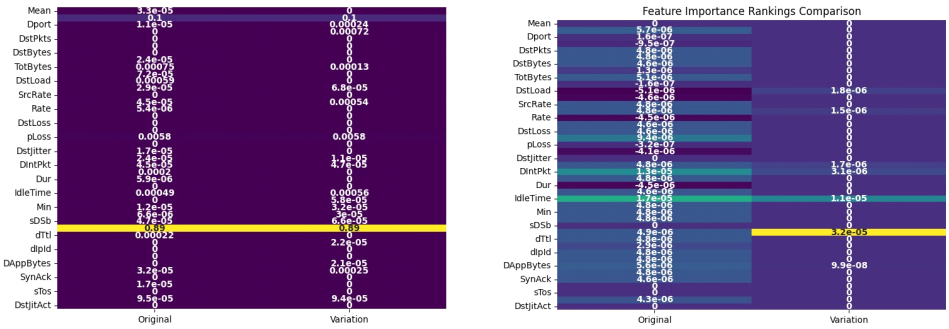
(a) Decision Tree (b) Random Forest

Fig. 2. Heatmap showing the comparison of the feature importance rankings between the original and the varied compared models of the decision tree and random forest in the WUSTL-2018 dataset scenario.



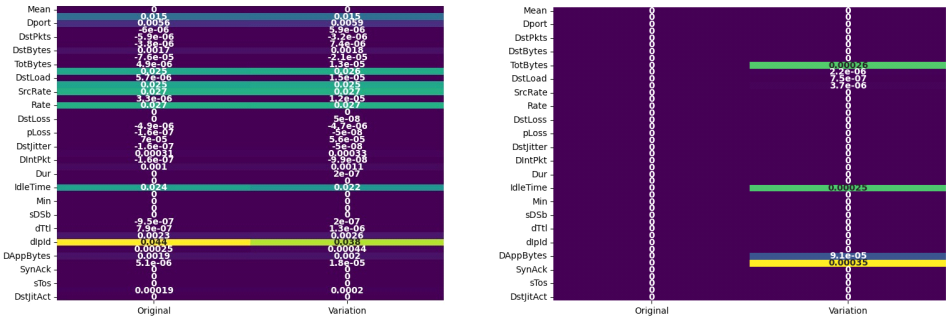
(a) Naive Bayes (b) Deep Neural Network

Fig. 3. Heatmap showing the comparison of the feature importance rankings between the original and the varied compared models of naive bayes and deep neural networks in the WUSTL-2018 dataset scenario.



(a) Decision Tree (b) Random Forest

Fig. 4. Heatmap comparing the feature importance rankings between the original and the varied compared models of the decision tree and random forest in the WUSTL-IIoT-2021 dataset scenario.



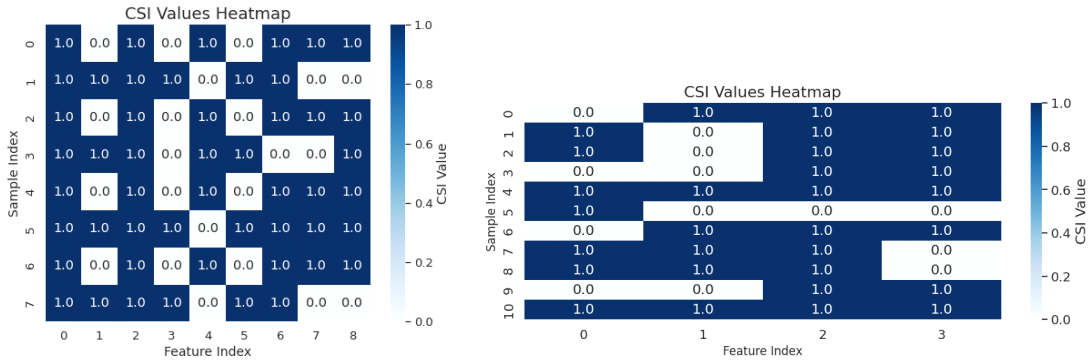
(a) Naive Bayes (b) Deep Neural Network

Fig. 5. Heatmap comparing the feature importance rankings between the original and the varied compared models of naive bayes and deep neural networks in the WUSTL-IIoT-2021 dataset scenario.

DNN algorithms. The decision tree and random forest algorithms demonstrated a high proportion of feature ranking stability over the other compared algorithms. The consistency in the heatmap color shows its level of stability with a few color variations in yellow and blue. It affirms the suitability of the tree algorithms as choice candidates for IIoT anomaly/intrusion detection. The proportion of variability demonstrated by the color contrasts exhibited by the naive bayes and DNN confirms its unsuitability for heterogeneous IIoT sensor data. Consequently, the consistency in the stability of the decision tree, particularly for the multiclass classification validates its applicability in a highly complex scenario like IIoT, in contrast to the instability displayed by the random forest, naive bayes, and DNN evidenced by the variability in coloration, especially for multi-class classification. The comparative analysis shows the performance of the evaluated models regarding the significance of the data features and their rankings in IIoT intrusion detection.

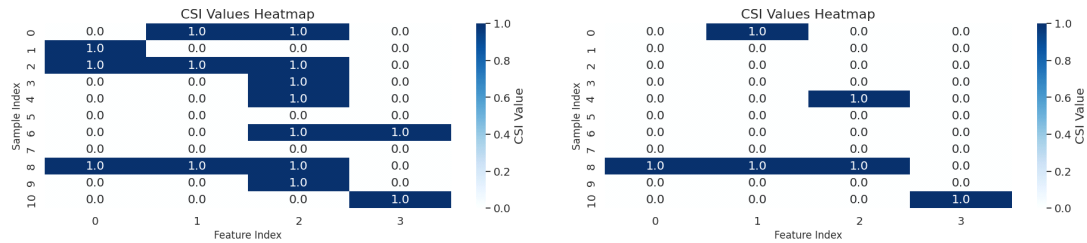
Consequently, Fig. 6 and Fig. 7 show the intensity of stability of the evaluated models. The CSI of the multi-class is considered due to varying data features and attack scenarios to show the consistency in stability observed as demonstrated by the tree algorithms. It confirms the aptness of the tree algorithms for intrusion in diverse heterogeneous IIoT networks[31].

A comparative analysis of the evaluated algorithms, as shown in Table 2, highlights the significance of the decision tree algorithm amongst the other compared classifiers. Despite all evaluated algorithms recording accuracy above 99%, the decision tree was outstanding in 1.82s train time for binary and 12.9s for multiclass in both scenarios. At the same time,



(a) Decision Tree (b) Random Forest

Fig. 6. CSI value heatmap showing the extent of stability exhibited by the decision tree and random forest algorithms.



(a) Naive Bayes (b) Deep Neural Network

Fig. 7. CSI value heatmap showing the extent of stability exhibited by the naive bayes and DNN algorithms.

Table 2. Comparative Analysis of the Performance of the Evaluated Algorithms

Model	WUSTL_2018			WUSTL-IIoT-2021		
	Train Time (s)	Feature Importance Permutation Time (s)	Accuracy (%)	Train Time (s)	Feature Importance Permutation Time (s)	Accuracy (%)
Decision Tree	**1.82**	**0.00046**	**1.0**	**12.9**	**0.00017**	**0.99**
Random Forest	28.14	259.20	1.0	144	1590.58	0.99
Naive Bayes	0.24	14.49	0.99	2.30	365.60	0.94
DNN	376.66	802.14	0.99	202.97	1491.65	0.93

it achieved feature importance permutation at 0.00046 in binary and 0.00017*s* multi-class scenarios.

V. Conclusion

Efficient monitoring of model stability in heterogeneous IIoT sensor data involves continuous data shift detection, assessing feature consistency, and tracking performance. It ensures adaptability and reliability in dynamic industrial settings. Regular monitoring is imperative to sustain model relevance and dependability. This research assesses ML classifier reliability by evaluating consistency across diverse data samples and iterations. CSI validates the applicability of the decision tree amongst other compared algorithms for IIoT anomaly/intrusion detection. Experimental outcomes offer actionable insights, empowering domain experts and minimizing operational risks and costs in IDS model selection. The CSI facilitates proactive model maintenance by analyzing evolving data's impact on behavior. Customizable thresholds align it with application needs, while interpretable insights enhance transparency. Real-time assessments make CSI pivotal

for reliable models in intricate IIoT ecosystems. Future research aims to explore CSI's broader applicability.

References

[1] N. Tariq, M. Asim, and F. A. Khan, "Securing SCADA-based critical infrastructures: Challenges and open issues," *Procedia Comput. Sci.*, vol. 155, pp. 612-617, 2019.

[2] S. V. B. Rakas, M. D. Stojanović, and J. D. Marković-Petrović, "A review of research work on network-based SCADA intrusion detection systems," *IEEE Access*, vol. 8, pp. 93 083-93 108, 2020.

[3] J. Gao, L. Gan, F. Buschendorf, et al., "Omni SCADA intrusion detection using deep learning algorithms," *IEEE Internet of Things J.*, vol. 8, no. 2, pp. 951-961, 2021. (https://doi.org/10.1109/JIOT.2020.3009180)

[4] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, pp. 1-22, 2019.

[5] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine learning-based network vulnerability analysis of industrial internet of things," *IEEE Internet of Things J.*, vol. 6, no. 4, pp. 6822-6834, 2019.

[6] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems," *IEEE Access*, vol. 7, pp. 46 595-46 620, 2019.

[7] P. Zeng and P. Zhou, "Intrusion detection in SCADA system: A survey," in *Intelligent Computing and Internet of Things*, Springer, pp. 342-351, 2018.

[8] L. A. C. Ahakonye, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Efficient classification of enciphered scada network traffic in smart factory using decision tree algorithm," *IEEE Access*, vol. 9, pp. 154 892-154 901, 2021.

[9] U. O. Obonna, F. K. Opara, C. C. Mbaocha, et al., "Detection of man-in-the-middle (MitM) cyber-attacks in oil and gas process control networks using machine learning algorithms," *Future Internet*, vol. 15, no. 8, p. 280, 2023. (https://doi.org/10.3390/fi15080280)

[10] L. A. C. Ahakonye, C. I. Nwakanma, J. M. Lee, and D.-S. Kim, "Agnostic CH-DT technique for SCADA network high-dimensional dataaware intrusion detection system," *IEEE Internet of Things J.*, vol. 10, no. 12, 2023. (https://doi.org/10.1109/JIOT.2023.3237797)

[11] P. Williams, I. K. Dutta, H. Daoud, and M. Bayoumi, "A survey on security in internet of things with a focus on the impact of emerging technologies," *Internet of Things*, vol. 19, p. 100564, 2022.

[12] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review," *Sensors*, vol. 23, no. 8, p. 4117, 2023.

[13] L. A. C. Ahakonye, C. I. Nwakanma, J. M. Lee, and D.-S. Kim, "Verifying the stability of tree algorithms on complex industrial internet of things dataset," in *Proc. KICS Summer Conf.*, 2023. [Online]. Available: https://journalhome.s3.apnortheast2.amazonaws.com/site/2023s/abs/0498OLYHF.pdf.

[14] S. Alkadi, S. Al-Ahmadi, and M. M. Ben Ismail, "Toward improved machine learning-based intrusion detection for internet of things traffic," *Computers*, vol. 12, no. 8, p. 148, 2023.

[15] L. A. C. Ahakonye, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "SCADA intrusion detection scheme exploiting the fusion of modified decision tree and chi-square feature selection," *Internet of Things*, vol. 21, p. 100 676, 2023.

[16] B. Yurdakul, *Statistical Properties of Population Stability Index*, Western Michigan University, 2018. [Online]. Available: https://scholarworks.wmich.edu/dissertations/3208

[17] A. Subbaswamy, R. Adams, and S. Saria, "Evaluating model robustness and stability to

dataset shift," in *Int. Conf. Artificial Intell. and Statistics*, PMLR, pp. 2611-2619, 2021.

[18] A. Becker and J. Becker, "Dataset shift assessment measures in monitoring predictive models," *Procedia Computer Sci.*, vol. 192, pp. 3391-3402, 2021.

[19] J. Ramzai, "Population stability index and characteristic stability index," in *PSI and CSI: Top 2 Model Monitoring Metric*, Towards Data Science, Aug. 2020.

[20] S. Cateni, V. Colla, and M. Vannucci, "Improving the stability of the variable selection with small datasets in classification and regression tasks," *Neural Process. Lett.*, pp. 1-26, 2022.

[21] C. I. Nwakanma, A. Zainudin, L. A. C. Ahakonye, G. O. Anyanwu, J. M. Lee, and D.-S. Kim, "Reliability analysis of modified random forest model for activity detection using F-Test," in *Proc. KICS Winter Conf.*, pp. 1112-1113, 2022.

[22] Github, *Population Stability Index*, 2018. [Online]. Available: https://mwburke.github.io/data%20science/2018/04/29/populationstabilityindex.html.

[23] M. Reckling, H. Ahrends, T.-W. Chen, et al., "Methods of yield stability analysis in longterm field experiments. A review," *Agronomy for Sustainable Development*, vol. 41, pp. 1-28, 2021.

[24] R. Taplin and C. Hunt, "The population accuracy index: A new measure of population stability for model monitoring," *Risks*, vol. 7, no. 2, p. 53, 2019.

[25] R. D. Riley and G. S. Collins, "Stability of clinical prediction models developed using statistical or machine learning methods," *arXiv preprint arXiv:2211.01061*, 2022.

[26] S. Cateni, V. Colla, and V. Iannino, "Improving the stability of variable selection for industrial datasets," *Neural Advances in Processing Nonlinear Dynamic Signals*, vol. 27, pp. 209-218, 2019.

[27] F. A. P. Peres, T. N. Peres, F. S. Fogliatto, and M. J. Anzanello, "Fault detection in batch processes through variable selection integrated to multiway principal component analysis," *J. Process Control*, vol. 80, pp. 223-234, 2019.

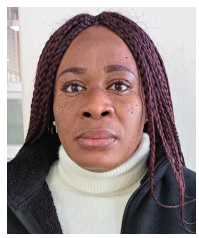
[28] S. Cateni, V. Colla, et al., "Improving the stability of wrapper variable selection applied to binary classification," *Int. J. Comput. Inf. Syst. Ind. Manag. Appl*, vol. 8, pp. 214-225, 2016.

[29] A. Lin, "*Examining distributional shifts by using population stability index (psi) for model validation and diagnosis*," URL http://www.lexjansen.com/wuss/2017/47_Final_Paper_PDF.pdf, 2017.

[30] M. A. Teixeira, T. Salman, M. Zolanvari, R. Jain, N. Meskin, and M. Samaka, "SCADA system testbed for cybersecurity research using machine learning approach," *Future Internet*, vol. 10, no. 8, p. 76, 2018.

[31] L. A. C. Ahakonye, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Trees bootstrap aggregation for detection and characterization of IoT-SCADA network traffic," *IEEE Trans. Industrial Informatics*, 2023. (https://doi.org/10.1109/TII.2023.3333438)

Love Allen Chijioke Ahakonye



2001 : B.Sc. Mathematics/ Computer Science, University of Port Harcourt, Nigeria

2016 : M.Sc. Information Technology, Federal University of Technology, Owerri, Nigeria

Mar. 2021~Current : Ph.D Scholar and Researcher, IT-Convergence Engineering, Kumoh National Institute of Technology, Korea

<Research Interests> AI application to IIoT SCADA for intrusion / anomaly detection, cyber-security, fault detection, and manufacturing execution system.

[ORCID:0000-0003-2840-1693]

Cosmas Ifeanyi Nwakanma

May 2005 : B.Eng. Electrical/ Electronics Engineering, Federal University of Technology, Owerri, Nigeria

Oct. 2012 : M.Sc. Information Technology, Federal University of Technology, Owerri, Nigeria

Feb. 2016 : MBA Project Management Technology, Federal University of Technology, Owerri, Nigeria

Feb. 2022 : Ph.D. IT-Convergence Engineering, Kumoh National Institute of Technology, Korea

Apr. 2009~Feb. 2019 : Lecturer, Department of Information Technology, Federal University of Technology, Owerri, Nigeria

Mar. 2022~Current : Senior Research Fellow, Kumoh National Institute of Technology, Korea

<Research Interests> Digital Twin and Metaverse, Explainable AI, Intrusion detection, Smart IoT Applications.

[ORCID:0000-0003-3614-2687]

Jae Min Lee

2005 : Ph.D. Electrical and Computer Engineering, Seoul National University, Seoul, Korea

2005~2014 : Senior Engineer, Samsung Electronics Engineering, Suwon, Korea

2015~2016 : Principal Engineer, Samsung Electronics Engineering, Suwon, Korea

2017~Current : Associate Professor, School of Electronic Engineering, Kumoh National Institute of Technology, Gyeongbuk, Korea

<Research Interests> Blockchain, TRIZ, Smart IoT convergence Application, industrial wireless control network, UAV, Metaverse.

[ORCID:0000-0001-6885-5185]

Dong-Seong Kim

2003 : Ph.D. Electrical and Computer Engineering, Seoul National University, Korea.

2003~2004 : Postdoctoral researcher, Cornell University, NY, USA

2007~2009 : Visiting Professor, The University of California, Davis, CA, USA

2004~Current : Professor, Kumoh National Institute of Technology (KIT), Gyeongbuk, Korea

2014~Current : Director, ICT Convergence Research Center, KIT, Gyeongbuk, Korea

2017~2022 : Dean, Industry-Academic Cooperation Foundation and Office of Research (ICT), KIT, Gyeongbuk, Korea

2022~Current : CEO, NSLab Co. Ltd., Korea

<Research Interests> Blockchain, Metaverse, Industrial IoT, real-time systems, industrial wireless control network, 5G+, and 6G.

[ORCID:0000-0002-2977-5964]