AN EMPIRICAL ANALYSIS OF ANOMALY DETECTION MODEL PARADIGMS UNDER HETEROGENEOUS IOMT ATTACK TRAFFIC

Visvakaanth KT
Department Of Computer Science
R.M.K Engineering College
Chennai, India
Visvakamal225566@gmail.com

Abstract— Hospitals deploy a wide range of heterogeneous Internet of Medical Things (IoMT) devices, each exhibiting distinct traffic patterns and operational behaviors. This heterogeneity presents challenges for anomaly-based intrusion detection systems (IDS), where traffic from diverse and segmented IoMT devices is ultimately aggregated or abstracted for centralized anomaly scoring. Although operational deployments incorporate device profiling and network segmentation, the statistical modeling assumptions at the anomaly detection layer play a critical role in detection behavior. In this work, we provide an empirical evaluation of global and cluster-aware Isolation Forest models: a global IF trained on heterogeneous IoMT traffic, and a cluster-aware IF trained on traffic subpopulations obtained through unsupervised clustering. Using the CCIoMT2024 dataset, we construct attack scenarios derived from legitimate IoMT traffic and evaluate how each configuration responds to device-level anomalies. This study focuses on the anomaly detection layer of an IDS pipeline and aims to assess how modeling granularity influences anomaly scoring behavior in heterogeneous IoMT environments.

Keywords— Internet of Medical Things (IoMT), anomaly detection, intrusion detection systems, Isolation Forest, heterogeneous network traffic, empirical evaluation

I. INTRODUCTION

Hospitals increasingly rely on Internet of Medical Things (IoMT) devices to monitor patients, administer treatments, and manage hospital operations. These devices exhibit highly heterogeneous traffic characteristics, with distinct feature distributions reflecting differences in device function, communication protocols, and operational roles. Despite this diversity, anomaly detection in hospital networks is often driven by centralized statistical models trained on aggregated or partially aggregated traffic representations, motivated by efficiency and deployment simplicity.

However, a centralized IDS may fail to detect malicious traffic from specific devices because anomalous patterns can be masked by normal traffic from other heterogeneous devices. For instance, a malicious data flow from an infusion pump may be interpreted as normal by a centralized IDS if other devices' traffic exhibits similar patterns or variability. This limitation poses significant Cybersecurity risks in hospital environments, where timely detection of threats is critical.

In this study, we empirically examine the behavior of Isolation Forest–based anomaly detection under heterogeneous IoMT traffic. Using the CCIoMT2024 dataset, we evaluate two modeling configurations: a global Isolation Forest trained on traffic from all devices, and cluster-specific Isolation Forests trained on traffic from groups of devices with similar characteristics. Malicious traffic resembling infusion-pump behavior is synthetically introduced to analyze how each configuration responds under identical attack conditions.

focusing on how modeling granularity influences anomaly detection behavior. Rather than proposing a new intrusion detection system, this work evaluates existing modeling approaches under controlled experimental conditions

This work provides an empirical analysis of the behavior and limitations of multiple anomaly detection modeling configurations under heterogeneous IoMT traffic. The contributions of this work are summarized as follows:

- We provide an empirical comparison between a global Isolation Forest model trained on heterogeneous IoMT traffic and cluster-aware Isolation Forest models trained on traffic subpopulations.
- We analyze how traffic heterogeneity and modeling assumptions affect anomaly detection behavior at the statistical scoring layer of an IDS pipeline.
- We present an experimental framework based on the CCIoMT2024 dataset for evaluating anomaly detection models under device-level attack scenarios.

II. RELATED WORK

Traditional hospital IDS systems operate over heterogeneous IoMT traffic, motivating the use of statistical anomaly detection models trained on diverse device data. While a wide range of approaches have been proposed, empirical comparisons that isolate the effects of modeling choices and granularity under controlled attack scenarios remain limited. To address this, we conduct an empirical study comparing multiple anomaly detection model configurations. Using the CCIoMT2024 dataset, we simulate malicious traffic derived from legitimate IoMT flows and analyze how different models fail under varying attack conditions. This study aims to provide empirical insight into how modeling assumptions and traffic heterogeneity influence anomaly detection behavior at the statistical scoring layer of an IDS pipeline.

III. METHODOLOGY

A.Dataset Description

The experiments in this work utilize the CCIoMT2024 dataset [1], which contains network traffic collected from a variety of Internet of Medical Things (IoMT) devices commonly found in hospital environments. Each network flow is represented by statistical features capturing packet timing, size, and protocol characteristics. Device identities in the dataset are anonymized; however, the traffic remains heterogeneous, reflecting diverse communication behaviors across different IoMT device categories. Some traffic streams exhibit continuous activity, while others show intermittent or burst-like transmission patterns. This heterogeneity mirrors real-world hospital network conditions and motivates the evaluation of anomaly detection models trained on aggregated and partitioned traffic representations.

B. Malicious Traffic Simulation

For empirical evaluation, selected traffic flows in the dataset were modified to introduce controlled anomalous behavior. The injected traffic was designed to resemble

communication patterns associated with infusion-pump–like devices, resulting in anomalies that remain statistically similar to legitimate IoMT traffic. These modified flows serve as controlled anomaly instances, enabling systematic analysis of how different anomaly detection models respond under identical conditions

.C. Global IDS Using Isolation Forest

A single Isolation Forest (IF) model [2] was trained using the full CCIoMT2024 dataset, resulting in a model learned from heterogeneous IoMT traffic. This configuration represents an aggregated training setting in which traffic from multiple device categories is modeled jointly. Controlled anomalous flows were subsequently introduced and evaluated by the model, with anomaly scores recorded over successive windows to analyze the model's response behavior under injected attack conditions.

D. Clustering of Device Traffic

To account for the heterogeneous nature of IoMT traffic, KMeans clustering [3] was applied to group network flows with similar statistical characteristics. Each cluster represents a subpopulation of traffic exhibiting comparable communication patterns, rather than explicit device identities, as the dataset is anonymized. Separate subsets of data were constructed for each cluster to support the evaluation of cluster-specific anomaly detection models. For controlled analysis, the cluster whose traffic characteristics most closely aligned with infusion-pump–like behavior was selected for targeted anomaly injection.

E. Cluster-Specific IDS Using Isolation Forest

A second Isolation Forest model was trained using only the traffic flows contained within the selected cluster, resulting in a model learned from a more homogeneous traffic subpopulation. The same set of controlled anomalous flows introduced in the aggregated-traffic experiments was evaluated using this model. Anomaly scores were recorded over successive windows to analyze how a model trained on clustered traffic responds to injected anomalies under identical conditions.

F. Analysis of Model Response Behavior

The behavior of different anomaly detection configurations was analyzed by examining their predictions and anomaly scores in response to the same set of controlled anomalous flows. Two primary indicators were considered:

(i) The window index at which a modified flow was first assigned an anomalous score exceeding a predefined threshold

(ii) The relative magnitude and temporal evolution of anomaly scores across successive windows. This analysis enables consistent examination of how models trained under different traffic representations respond to identical injected anomalies.

IV. RESULTS

A. Anomaly Scoring Behavior of the Aggregated-Traffic Model

The Isolation Forest model trained on aggregated heterogeneous IoMT traffic was evaluated using controlled anomalous flows introduced into the CCIoMT2024 dataset. For each modified flow, anomaly predictions and scores were recorded across successive observation windows. Table I reports the first window index at which the anomaly score crossed the decision threshold for representative flows. If no threshold crossing occurred within the 15-window observation period, the result is indicated accordingly. These results illustrate variability in how quickly injected anomalies manifest in the anomaly scores when evaluated under an aggregated training configuration

.

Temporal Dynamics of Anomaly Scores:

To generate controlled anomalous flows, packet-level features of selected traffic were incrementally modified over successive observation windows. SYN, RST, and FIN counts were increased linearly to simulate progressive deviations, while ACK counts were gradually decreased to introduce subtle variations. Early windows often remained close to the nominal feature distribution which explains why anomaly scores did not exceed the threshold immediately in some flows. As feature values gradually diverge in subsequent windows, the model eventually assigns anomalous scores in later windows.

For some flows, anomaly scores did not exceed the threshold within the 15-window observation period. This occurs because, for these flows, the feature modifications were not sufficiently divergent relative to the aggregated heterogeneous traffic distribution. In other words, the injected anomalies remained statistically similar to the nominal traffic for the entire observation window, which explains the absence of threshold crossings for these flows.

Flow Index	**First Threshold Crossing (Window)**
5	5
18	1
35	6
57	3
74	1
92	—
110	5
145	2

Flow Index	First Threshold Crossing (Window)
180	—
215	5

B. Anomaly Scoring Behavior of the Cluster-Specific Model

The cluster-specific Isolation Forest (IF) model was trained exclusively on a subset of flows representing similar traffic characteristics. The same controlled anomalous flows were tested on this model. Table II summarizes the first window index at which the anomaly score crossed the decision threshold for representative flows. If no threshold crossing occurred within the 15-window observation period, the result is indicated accordingly.

Temporal Dynamics of Anomaly Scores:

The cluster-specific Isolation Forest was trained on a subset of flows representing similar traffic patterns. Because the model only sees this narrower distribution, feature deviations introduced in the controlled anomalous flows become statistically significant more quickly. Early windows often exhibit sufficient divergence from the cluster's nominal behavior to trigger an anomaly score above the detection threshold. This explains why the first threshold crossings occur in earlier windows for many flows.

Although the cluster-specific model responds quickly to feature deviations, some flows reach the anomaly threshold in fewer windows than others because For some flows, the feature modifications are still within the natural variability of the cluster-specific traffic. Even though the model is trained on a more homogeneous subset, these anomalies do not deviate enough from the learned distribution to trigger an alert.

Flow Index	First Threshold Crossing (Window)
5	3
18	1
35	2
57	2
74	2
92	1
110	1
145	3
180	1
215	2

.

V. DISCUSSION

The results illustrate how modeling choices influence anomaly detection in heterogeneous IoMT traffic. When an Isolation Forest model is trained on aggregated traffic, some injected anomalies remain close to the overall nominal traffic distribution in early observation windows, delaying or preventing threshold crossings. This behavior highlights that heterogeneity in device traffic can affect how quickly and reliably anomalous flows are assigned high anomaly scores, even when the deviations are systematically introduced.

In the homogeneous configuration, the Isolation Forest model was trained on a subset of traffic exhibiting similar statistical patterns. By focusing on flows with comparable characteristics, deviations introduced in the anomalous flows were reflected more prominently in the anomaly scores. As a result, threshold crossings often occurred in earlier observation windows for these flows, and anomalies that remained subtle in the aggregated traffic scenario were more likely to be assigned anomalous scores within the observation period.

From a practical perspective, these observations highlight how modeling choices—such as training on traffic subsets with similar characteristics—can influence the timing and sensitivity of anomaly detection in hospital networks. Grouping similar IoMT flows may affect how deviations are reflected in anomaly scores, which could inform future exploration of scalable, device-aware IDS configurations.

However, this study has limitations. The malicious traffic was synthetically generated by modifying existing flows, which may not fully capture the complexity of real-world attacks. Additionally, the number of clusters and the choice of clustering algorithm may influence detection performance. Future work will include evaluating additional anomaly detection approaches, such as the ADTK toolkit, as well as exploring adaptive clustering, online learning, or supervised approaches when labeled attack data is available.

VI. CONCLUSION

This paper presented an empirical investigation of anomaly detection approaches for heterogeneous IoMT traffic in hospital environments. Using the CCIoMT2024 dataset, controlled anomalous flows were introduced and evaluated with Isolation Forest models trained on both aggregated traffic and traffic subsets identified through clustering. The

results highlight how modeling assumptions and traffic heterogeneity influence anomaly scoring behavior, including cases where certain flows remain close to normal distributions and evade detection. Future work will extend this study to additional anomaly detection methods, including the ADTK toolkit, and explore adaptive or supervised approaches to improve detection of complex real-world attacks.

Experimental results reveal that the behavior of anomaly detection models varies depending on the training configuration and the characteristics of the traffic. In the aggregated-traffic (heterogeneous) model, some malicious flows remained statistically similar to normal traffic in early observation windows, which delayed or prevented detection. Conversely, the cluster-specific (homogeneous) model detected deviations more rapidly in certain flows because the training data captured more localized patterns. However, even the homogeneous model occasionally failed to flag anomalies quicker when the injected deviations were subtle relative to the cluster's distribution.

These findings highlight the challenges of modeling heterogeneous IoMT traffic for anomaly detection. They suggest that both aggregated and cluster-aware approaches have limitations depending on the statistical divergence of anomalies from the nominal traffic. Incorporating clustering or other traffic-aware strategies can help make anomaly detection more sensitive to device-specific patterns without imposing excessive resource demands.

REFERENCES

[1] C.C.IoMT Research Group, *"CCIoMT2024: A Comprehensive Dataset for Internet of Medical Things Traffic Analysis,"* 2024. [Online]. Available: https://www.unb.ca/cic/datasets/cc-iomt-2024.html.

[2] F. T. Liu, K. M. Ting, and Z.-H. Zhou, *"Isolation Forest,"* in *Proceedings of the IEEE International Conference on Data Mining (ICDM),* 2008, pp. 413–422.

[3] MacQueen, J. Some Methods for Classification and Analysis of Multivariate Observations. Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability.