DOI: 10.1109/SVCC65277.2025.11133650

FeatNet-IDS: Anomaly Detection based-Features for Industrial Internet of Things Systems

Wael Alsabbagh[1,2], Bahij Sayegh[1], Chaerin Kim[1,2] and Peter Langendörfer[1,2]
[1]*Brandenburg University of Technology Cottbus-Senftenberg, Cottbus, Germany*
[2]*IHP – Leibniz-Institut für innovative Mikroelektronik, Frankfurt (Oder), Germany*
E-mail: (Wael.alsabbagh, Bhij.sayegh, Chaerin.kim, peter.Langendoerfer)@b-tu.de

***Abstract*—Anomaly detection is critical for securing Industrial Internet of Things (IIoT) systems against evolving cyber threats. This paper introduces FeatNet-IDS, an enhanced Intrusion Detection System (IDS) for MQTT-based IIoT environments. FeatNet-IDS combines advanced feature selection and machine learning techniques to improve anomaly detection accuracy, efficiency, and interpretability. Evaluated on a domain-specific dataset of MQTT-related attacks, including control logic injection, the framework achieves 92.3% accuracy, 91.5% F1-score, and 96.8% ROC AUC, with a low false alarm rate of 2.73%. By emphasizing feature stability and importance, FeatNet-IDS outperforms or matches state-of-the-art methods, demonstrating robustness and transparency. Practical deployment implications are discussed, with future work addressing dataset expansion, hyperparameter tuning, and advanced ensemble approaches. The dataset and framework codes are publicly available to support further research.**

***Index Terms*—IIoT; MQTT Protocol; Cyberattacks; Cybersecurity, Anomaly Detection**

I. Introduction

The Industrial Internet of Things (IIoT) is revolutionizing industrial operations by enabling enhanced connectivity, efficiency, and adaptability [1], [2]. This transformation heavily relies on the Message Queuing Telemetry Transport (MQTT) protocol [7], a lightweight, publish-subscribe communication standard optimized for real-time and low-bandwidth scenarios. MQTT facilitates seamless communication among IIoT devices such as smart sensors, programmable logic controllers (PLCs), and human-machine interfaces (HMIs), forming the backbone of many modern industrial systems.

Despite its benefits, MQTT's growing adoption has exposed IIoT systems to significant security risks. The protocol's simplicity and lack of comprehensive built-in security measures make it vulnerable to various cyber threats [21], [22], such as Man-in-the-Middle (MitM) [2], [4], Denial of Service (DoS) [8], [9], control logic injection [2], [3], and many others. These vulnerabilities are particularly concerning in IIoT systems, where disruptions can lead to operational downtime, financial losses, or even physical harm.

To mitigate these risks, there is an urgent need for effective Intrusion Detection Systems (IDS) tailored to the unique characteristics of MQTT-based IIoT environments. Machine learning has emerged as a promising tool for enhancing IDS capabilities by analyzing complex patterns in network traffic to detect anomalies. However, existing approaches often face practical challenges, such as a reliance on synthetic datasets, limited scalability, and insufficient interpretability for real-world deployment.

This paper introduces *FeatNet-IDS*, an enhanced framework designed to address these challenges and secure MQTT-based IIoT systems. *FeatNet-IDS* combines advanced feature selection techniques with machine learning models to deliver high accuracy, efficiency, and interpretability in anomaly detection. Unlike many existing studies, this framework is grounded in real-world industrial settings, utilizing a domain-specific dataset of MQTT-related attacks. Data was collected from a Fischertechnik test-bed[1], replicating operational IIoT conditions to ensure practicality and scalability.

The proposed framework follows a structured methodology, including:

- **Data Collection:** Capturing network traffic under normal and attack scenarios, with a focus on control logic injection attacks.
- **Feature Engineering:** Transforming raw packet data into structured datasets using domain-specific techniques to enhance relevance.
- **Data Preprocessing:** Applying feature selection and normalization to optimize data for machine learning models.
- **Model Development:** Training and evaluating machine learning algorithms for anomaly detection in MQTT traffic.
- **Performance Evaluation:** Assessing the framework's effectiveness using metrics such as accuracy, F1-score, and Receiver Operating Characteristic - Area Under the Curve (ROC AUC).

FeatNet-IDS achieves competitive results, including a mean accuracy of 92.3%, an F1-score of 91.5%, and a ROC AUC of 96.8%, with a low false alarm rate of 2.73%. These metrics highlight the framework's robustness and interpretability, outperforming or matching state-of-the-art methods. Moreover, the emphasis on real-world experimentation underscores its practicality for securing IIoT systems. Additionally, *FeatNet-IDS*'s code [24] and dataset [25] are publicly available, fostering further research and development in this domain.

The rest of this paper is structured as follows: Section II reviews related work, while Section III outlines the experi-

[1]https://www.fischertechnik.de/de-de/industrie-und-hochschulen/technische-dokumente/simulieren/lernfabrik-4-0-24v

mental setup. The proposed *FeatNet-IDS* approach is detailed in Section IV. Section V presents the results and evaluation of our framework, followed by a discussion in Section VI. Finally, Section VII concludes the paper.

II. Related Work

A variety of methodologies, including Federated Learning (FL), Machine Learning (ML), Deep Learning (DL), Deep Reinforcement Learning (DRL), and Graph-based Anomaly Detection (GBAD), have been investigated to enhance the security of IIoT systems. Network anomalies, as highlighted by [10], disrupt normal behavior through abrupt changes, which can often be detected using statistical and signal-processing techniques. [11] underscores the growing complexity of IIoT network traffic, necessitating robust and scalable anomaly detection solutions. Hamamoto et al. [12] proposed a hybrid approach that combines genetic algorithms and fuzzy logic for anomaly detection. However, scalability in dynamic environments remains a significant challenge. Naseer et al. [13] employed Deep Neural Networks (DNNs) for high-dimensional anomaly detection, achieving high accuracy but facing issues related to computational overhead and interpretability. Nagaraja et al. [14] introduced similarity-based feature transformation for dimensionality reduction, which enhanced detection performance but struggled to adapt to IIoT-specific constraints. Similarly, mutual information-based feature selection methods, as described by [15], optimized detection pipelines but were sensitive to noise and required extensive parameter tuning. Fuzzy-enhanced systems, discussed by D'Angelo [16], dynamically adjusted detection thresholds to handle noisy traffic. However, these systems often relied on manual rule calibration, limiting their generalizability across diverse attack scenarios.

In contrast, our proposed *FeatNet-IDS* framework directly addresses these challenges by grounding its methodology in real-world industrial environments. Utilizing data collected from a Fischertechnik test-bed, it replicates operational IIoT conditions to ensure realism. By integrating advanced feature selection with machine learning, the framework strikes a balance between accuracy, interpretability, and efficiency, specifically tailored for MQTT-based IIoT systems. This practical and scalable solution bridges the gap between theoretical research and real-world applications, significantly enhancing the security of IIoT networks.

III. Experimental Setup

The Fischertechnik Training Factory Industry 4.0 24V serves as a modular industrial test-bed that replicates real-world manufacturing processes, as shown in Figure 1.

This test-bed incorporates an S7-1500 PLC and features multiple interconnected modules, including a storage and retrieval station, vacuum gripper robot, high-bay warehouse, multi-processing station, sorting line with color detection, and environmental sensors. These components simulate industrial workflows such as production, assembly, and quality control, providing a realistic environment for studying IIoT operations.

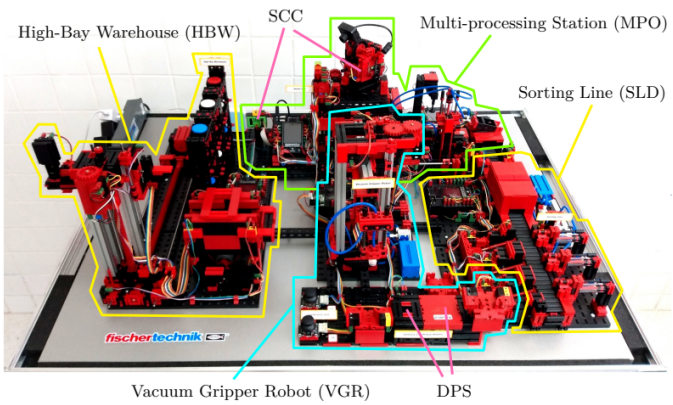

Fig. 1: Fischertechnik Lernfabrik 4.0 24V, adapted from [23].

The system employs MQTT for communication, with an IoT gateway converting data to Open Platform Communications Unified Architecture (OPC-UA) for seamless integration with Industrial Control Systems (ICS). Additionally, Near Field Communication (NFC) technology is used for workpiece tracking, while environmental sensors enable real-time monitoring, mirroring the complexity of operational IIoT environments.

The Fischertechnik test-bed was chosen to validate the proposed *FeatNet-IDS* framework in a realistic industrial environment. Unlike synthetic datasets or simulations, it replicates the intricate communication patterns and complexities of real-world IIoT systems, ensuring applicability and robustness. This setup enabled the collection of high-quality network traffic data under normal and attack scenarios, particularly focusing on control logic injection attacks. Its modular design facilitated controlled experiments, capturing diverse data from NFC tracking and environmental sensors. This enriched dataset was instrumental in developing *FeatNet-IDS* and enhancing its ability to detect subtle anomalies in MQTT-based IIoT environments.

IV. FeatNet-IDS Approach

The *FeatNet-IDS* framework is designed to address the challenges of anomaly detection in IIoT networks by integrating advanced feature extraction techniques with robust machine learning models. This section describes its architecture, as illustrated in Fig. 2, and explains its three key stages: data collection, feature extraction, and model training and evaluation.

A. Data Collection

The first stage focuses on collecting network traffic data from IIoT systems, specifically the Fischertechnik test-bed. A network switch equipped with a remote packet capture tool (Wireshark[2]) was employed to monitor traffic non-intrusively during both normal and anomalous operations.

[2]https://www.wireshark.org/

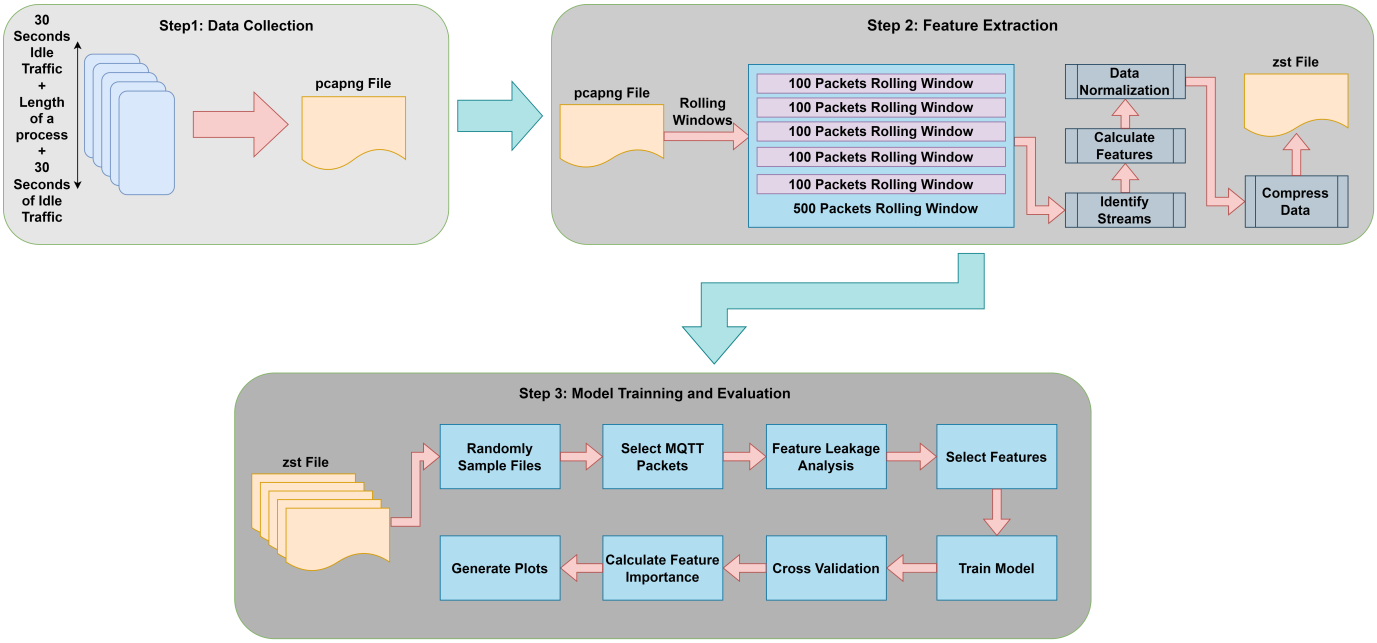

Fig. 2: Overview of the *FeatNet-IDS* Framework.

*1) **Normal Operation Traffic**:* To establish a baseline for anomaly detection, network traffic was captured during normal operations. This included both idle states and active processes such as workpiece ordering and stock movement. Traffic for each workpiece type and process was recorded 50 times, resulting in a total of 600 instances of normal traffic. This setup closely mirrors realistic IIoT operational conditions.

*2) **Anomalous Operation Traffic**:* To assess the system's capability to detect malicious behavior, controlled attack simulations were performed. Drawing on prior studies [2]–[6], attacks such as control logic injections and data injections were simulated, producing 360 instances of anomalous traffic. These scenarios were carefully designed to encompass diverse and realistic attack patterns.

B. Feature Extraction

FeatNet-IDS transforms raw network traffic into actionable insights through feature extraction. The extracted features fall into four main categories: packet-level, flow-based, statistical dispersion measures, and protocol-specific.

*1) **Packet-Level Features**:* Packet-level features focus on detecting protocol-specific anomalies and attacks. Using Scapy[3], detailed features were extracted from Transmission Control Protocol/Internet Protocol (TCP/IP) and MQTT traffic.

- **TCP/IP Features:** includes packet size, TCP flags, and flow duration. These features detect attacks such as Synchronization (SYN) flooding and session hijacking. Specific analyses include:
  - *TCP Flag Analysis:* examines the state of TCP flags (e.g., SYN, FIN, RST) for incomplete handshakes or abnormal patterns.
  - *Flow Duration and Packet Rate:* variations in these metrics reveal attacks like DoS.
- **MQTT Features:** focuses on message frequency, Quality of Service (QoS) levels, and message sizes. Key analyses include:
  - *Message Type and Frequency:* tracks unusual exchanges of *CONNECT*, *PUBLISH*, and *SUBSCRIBE* messages.
  - *Message Size Distribution:* detects anomalies in payload size indicative of protocol abuse.

Table I summarizes the packet-level features, essential for detecting unauthorized access and traffic manipulation.

*2) **Flow-Based Features**:* Flow-based features capture long-term traffic behaviors, enabling detection of stealthy attacks. Key features include:

- **Flow Duration and Directionality:** Distinguishes bidirectional and unidirectional flows.
- **Packet and Byte Rates:** Highlights traffic spikes or drops, revealing DoS or data siphoning.
- **Temporal Analysis:** Irregularities in packet timing indicate covert channels or delays.

Table II lists the engineered flow-based features used in *FeatNet-IDS*.

*3) **Statistical Dispersion Measures**:* Advanced statistical measures, such as Coefficient of Variation (CV), Interquartile Range (IQR), and Moving Range (MR), are employed to detect subtle traffic anomalies. These metrics effectively reveal stealthy attacks by identifying irregular traffic variability and outliers.

*4) **Protocol-Specific Features**:* Protocol-specific features target vulnerabilities in IIoT protocols. Examples include:

[3]https://scapy.net/

TABLE I: Packet-Level features to detect protocol-specific anomalies and attacks

Category	Feature Name	Description	Anomaly Detection Purpose
4*Basic	packet_size	Total packet size including headers	Data exfiltration detection
	inter_arrival_time	Time between consecutive packets	Timing attack detection
	source_ip_address	Source IP of the packet	Source verification
	destination_ip_address	Destination IP of the packet	Unauthorized communication
2*Port	source_port	Source port number	Service identification
	destination_port	Destination port number	Unauthorized service detection
8*TCP Flags	tcp_syn_flag	Synchronization flag	Connection initiation analysis
	tcp_ack_flag	Acknowledgment flag	Connection state tracking
	tcp_fin_flag	Finish flag	Connection termination patterns
	tcp_rst_flag	Reset connection flag	Abnormal terminations
	tcp_psh_flag	Push data flag	Data flow analysis
	tcp_urg_flag	Urgent data flag	Priority handling verification
	tcp_ece_flag	ECN-Echo flag	Congestion monitoring
	tcp_cwr_flag	Congestion Window Reduced	Network stress analysis
4*TCP State	tcp_payload_size	TCP payload length	Data volume analysis
	tcp_window_size	Flow control window size	Flow control verification
	tcp_sequence_number	Packet sequence number	Sequence attack detection
	tcp_acknowledgment_number	Acknowledgment number	State tracking
2*Link Layer	source_mac_address	Source MAC address	Device authentication
	destination_mac_address	Destination MAC address	Network topology validation
3*MQTT Basic	is_mqtt	MQTT packet indicator	Protocol verification
	mqtt_message_type	Type of MQTT message	Command pattern analysis
	mqtt_message_timestamp	Message timing	Temporal analysis
2*MQTT QoS	mqtt_qos_level	Quality of Service level	Service level verification
	mqtt_dup_flag	Duplicate packet flag	Message integrity
2*MQTT Session	mqtt_retain_flag	Message retention flag	Broker behavior analysis
	mqtt_clean_session_flag	Session cleanup indicator	Session management
3*MQTT Will	mqtt_will_flag	Last Will indicator	Connection monitoring
	mqtt_will_qos	Will message QoS	Service assurance
	mqtt_will_retain	Will message retention	Broker configuration
2*MQTT Content	mqtt_topic	MQTT topic string	Access pattern analysis
	mqtt_payload_size	MQTT payload size	Data volume monitoring

- **TCP SYN/FIN Ratios:** monitors connection patterns for scanning or hijacking attempts.
- **MQTT Publish-Subscribe Ratios:** highlights abnormal subscriptions or false data injections.

C. *Model Training and Evaluation*

The final stage focuses on training machine learning models using the extracted features. A range of classifiers, including decision trees, random forests, and deep neural networks, are evaluated to determine the optimal model for anomaly detection. The models are assessed using the following key performance metrics:

- **Accuracy:** quantifies the overall correctness of predictions, providing a general measure of model performance.
- **Precision and Recall:** assess the model's ability to correctly identify positive instances (precision) and its capacity to detect all relevant instances (recall), ensuring a balance between sensitivity and specificity.
- **F1-Score:** combines precision and recall into a single metric, offering a harmonic mean that ensures a balanced evaluation of both measures.

FeatNet-IDS undergoes rigorous testing across a variety of attack scenarios to validate its robustness and generalizability. This ensures the framework's adaptability to a wide range of IIoT systems and its capacity to effectively detect and mitigate emerging threats.

V. Results and Evaluation

This section presents the evaluation of the *FeatNet-IDS* framework, providing both quantitative and qualitative analyses. The assessment covers feature stability, feature selection, classification performance, and anomaly detection across various metrics. These evaluations demonstrate the strengths of the model while identifying areas for further improvement.

TABLE II: Engineered Flow Features

Category	Feature Name	Description	Anomaly Detection Purpose
3*Flow Identification	flow_id	Unique identifier for each flow	Tracks flows for detailed monitoring
	flow_duration	Duration of the flow in seconds	Detects prolonged or short-lived flows
	source_destination_ratio	Ratio of source to destination packets	Identifies asymmetric communication
4*Basic Flow Metrics	total_packets	Number of packets in the flow	Detects abnormal packet counts
	total_bytes	Total bytes transferred in the flow	Identifies large data transfers
	packet_rate	Packets per second in the flow	Tracks traffic spikes
	byte_rate	Bytes per second in the flow	Monitors bandwidth usage
7*Inter-arrival Time	mean_inter_arrival_time	Average time between packets	Highlights timing irregularities
	inter_arrival_time_variance	Variance of inter-arrival times	Captures timing instability
	inter_arrival_time_std_dev	Standard deviation of inter-arrival times	Measures spread in timings
	inter_arrival_time_range	Range of inter-arrival times	Tracks extreme timing deviations
	inter_arrival_time_25th_percentile	First quartile of inter-arrival times	Detects small timing anomalies
	inter_arrival_time_50th_percentile	Median of inter-arrival times	Central tendency in timing
	inter_arrival_time_75th_percentile	Third quartile of inter-arrival times	Highlights larger timing anomalies
2*Traffic Patterns	burst_count	Number of bursts (rapid packet sequences)	Identifies bursty traffic behaviour
	silence_count	Number of silent periods in traffic	Tracks traffic inactivity
7*Packet Size	average_packet_size	Mean size of packets in the flow	Monitors typical packet size
	packet_size_variance	Variance in packet sizes	Captures variability in size
	packet_size_std_dev	Standard deviation of packet sizes	Tracks spread in packet sizes
	packet_size_range	Range of packet sizes in the flow	Detects extreme packet sizes
	packet_size_25th_percentile	First quartile of packet sizes	Identifies smaller packet anomalies
	packet_size_50th_percentile	Median size of packets	Captures typical packet size
	packet_size_75th_percentile	Third quartile of packet sizes	Tracks larger packet sizes
3*Distribution Metrics	packet_size_z_score	Normalized score of packet size	Detects statistical outliers
	inter_arrival_time_z_score	Normalized score of inter-arrival times	Highlights timing outliers
	packet_size_entropy	Entropy of packet size distribution	Measures randomness in size

A. *Evaluation Metrics*

We assess the model's performance using the following standard metrics:

1) ***Accuracy****:* Accuracy measures the proportion of correctly classified instances out of all instances:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

where TP, TN, FP, and FN represent true positives, true negatives, false positives, and false negatives, respectively.

2) ***Precision****:* Precision quantifies the proportion of true positive predictions among all positive predictions:

$$\text{Precision} = \frac{TP}{TP + FP} \tag{2}$$

3) ***Recall****:* Recall measures the proportion of actual positives correctly identified by the model:

$$\text{Recall} = \frac{TP}{TP + FN} \tag{3}$$

4) ***F1-Score****:* The F1-score is the harmonic mean of precision and recall:

$$\text{F1-Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{4}$$

5) ***ROC AUC****:* The ROC AUC evaluates the model's ability to distinguish between classes at various decision thresholds:

$$\text{ROC AUC} = \int_0^1 \text{TPR}(FPR)\, d(\text{FPR}) \tag{5}$$

where TPR and FPR represent the true positive rate and false positive rate, respectively.

6) ***False Alarm Rate (FAR)****:* The FAR is the proportion of false positive predictions relative to all negative instances:

$$\text{FAR} = \frac{FP}{FP + TN} \tag{6}$$

For *FeatNet-IDS*, the FAR was computed at 2.73%, demonstrating its effective minimization of false alarms.

B. *Experimental Results*

1) ***Feature Stability Analysis****:* The stability of the features selected by the model is evaluated by assessing their consistency across multiple data subsamples. Table III presents the stability statistics, showing a mean stability score of 0.974, indicating that most features contribute consistently to the model.

TABLE III: Feature Stability Statistics for *FeatNet-IDS*

Metric	Value
Number of Features Analyzed	138
Mean Stability Score	**0.974**
Standard Deviation	1.936
Minimum Stability	0.0
Maximum Stability	15.312
Undefined Scores	4

*2) **Feature Importance Analysis**:* Feature importance analysis is essential for identifying the attributes that most influence the model's predictions. Table IV presents the top 10 features for anomaly detection, ranked by their contribution to the model's performance within *FeatNet-IDS*.

TABLE IV: Top 10 Feature Importance Rankings for *FeatNet-IDS*

Feature	Importance Score
iat_skewness_100	1.756
destination_ip_address	1.538
mean_inter_arrival_time_500	1.379
flow_duration_500	1.279
inter_arrival_time_25th_percentile_100	1.436
packet_arrival_rate_mean_100	1.337
burst_count_500	1.610
inter_arrival_time_range_500	1.552
iat_rolling_entropy_100	1.759
packet_rate_500	1.220

Table IV shows that features such as *iat_skewness_100*, *destination_ip_address*, and *burst_count_500* exhibit high importance scores, indicating that anomalies in traffic flow distribution, destination IP address patterns, and burst traffic behavior are key indicators for the model. Other notable features, including *mean_inter_arrival_time_500* and *iat_rolling_entropy_100*, highlight the significance of timing and unpredictability in detecting network anomalies. Overall, these features contribute significantly to the framework's ability to identify subtle deviations in IIoT systems.

*3) **Cross-Validation Metrics**:* The Cross-Validation (CV) metrics presented in Table V highlight the FeatNet-IDS framework's consistent and robust performance across multiple validation folds.

TABLE V: CV Metrics for *FeatNet-IDS*

Metric	Mean	Std. Dev.	Min	Max
Accuracy	0.923	0.015	0.894	0.935
Precision	0.921	0.075	0.774	0.984
Recall	0.915	0.029	0.867	0.944
F1-Score	0.915	0.034	0.851	0.949
ROC AUC	0.968	0.021	0.930	0.984

Our model achieves a high mean accuracy of 92.3%, with a narrow standard deviation of 1.5%, indicating stable performance across different subsets of the data. Precision and recall scores, with means of 92.1% and 91.5%, respectively, show that the model maintains a good balance between identifying true positive anomalies and minimizing false negatives. The F1-score, combining precision and recall, further supports the framework's effectiveness in anomaly detection, with a mean value of 91.5%. The ROC AUC score of 96.8% demonstrates the model's strong ability to distinguish between normal and anomalous traffic across varying thresholds. These results underscore the reliability of *FeatNet-IDS* in real-world IIoT anomaly detection scenarios. Figures 3, and 4 present graphical representations of these cross-validation results.

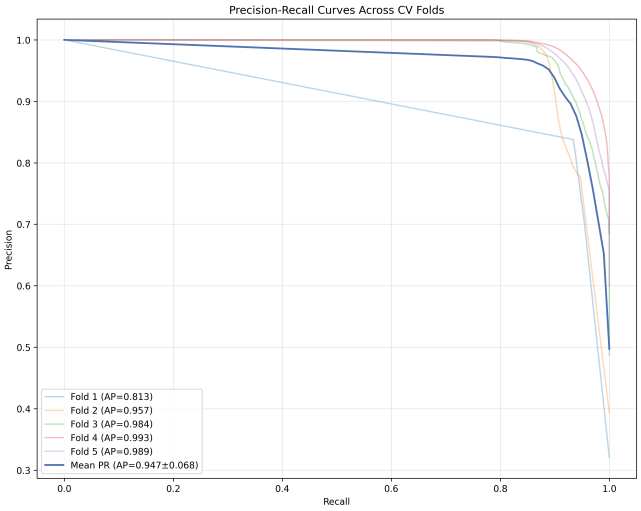

Fig. 3: Precision-Recall Curves Across CV Folds

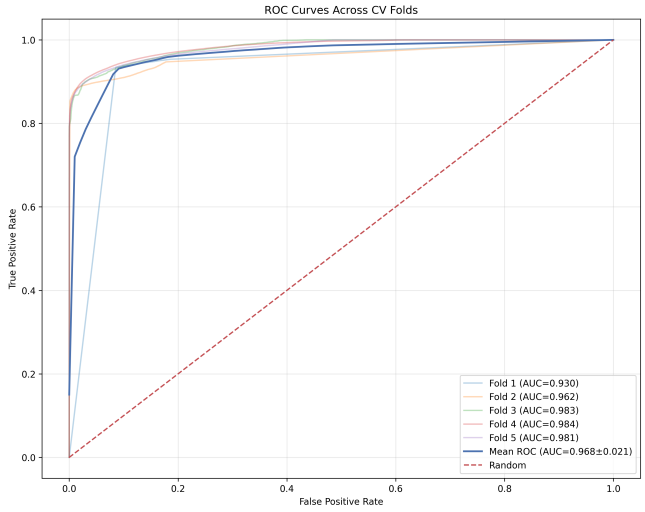

Fig. 4: ROC Curves Across CV Folds

*4) **Confusion Matrix Analysis**:* The normalized confusion matrix, presented in Figure 5, provides a detailed overview of the model's classification performance. The low False Alarm Rate (FAR) of 2.73% demonstrates *FeatNet-IDS*'s strong capability in correctly classifying normal and anomalous traffic while minimizing false positives. This result emphasizes the model's reliability in identifying genuine anomalies without triggering excessive false alarms, a critical factor for anomaly detection in IIoT systems where false positives can lead to operational inefficiencies.

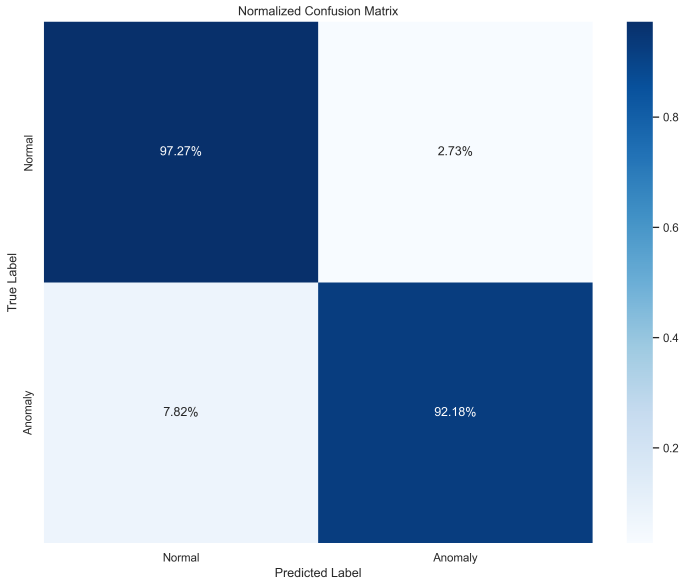

Fig. 5: Normalized Confusion Matrix in *FeatNet-IDS*

C. *Performance Evaluation*

1) ***General Performance****:* The *FeatNet-IDS* model demonstrates robust performance, achieving a mean accuracy of 92.3% and an F1-score of 91.5%. The ROC AUC of 96.8% highlights the model's excellent discriminatory capability.

2) ***False Alarm Rate****:* With a FAR of 2.73%, the model effectively minimizes false alarms, which is critical in anomaly detection, where false positives can incur significant operational costs.

3) ***Feature Stability and Importance****:* The feature stability analysis shows that the selected features are consistent across different data subsamples, with a high mean stability score of 0.974. Key features, such as '*iat_skewness_100*' and '*destination_ip_address*', provide insights into the model's interpretability.

D. *Limitations and Challenges*

Despite the strong overall performance of *FeatNet-IDS*, there are some challenges that need to be addressed. The observed variability in performance across CV folds suggests that further refinement in hyperparameter tuning is required. Such fine-tuning could lead to improved consistency and enhance the model's robustness, particularly in scenarios involving imbalanced data or varying environmental conditions. By addressing these challenges, the model's anomaly detection performance could be made more reliable and effective across diverse situations.

VI. Comparison and Discussion

This section evaluates the performance of *FeatNet-IDS* in comparison to existing methods, focusing on key metrics, feature selection approaches, and an analysis of its strengths and limitations. Table VI summarizes the evaluation metrics we used in our comparison.

FeatNet-IDS demonstrates competitive performance across all evaluation metrics, achieving an ROC AUC of 0.968 and an F1-score of 0.915. While it slightly lags behind [17] in ROC AUC and F1-score, it outperforms the other methods in balancing precision (0.921) and recall (0.915). Its FAR of 2.73% is among the lowest, suggesting high reliability in its anomaly detection capability.

The feature selection strategy employed in *FeatNet-IDS* focuses on stability and importance, yielding a mean stability score of 0.974. Key features such as *iat_skewness_100* have been identified as critical predictors. This strategy helps reduce computational overhead while maintaining a high level of model interpretability, making it well-suited for scalable anomaly detection. However, some features like *mqtt_message_timestamp* exhibit undefined stability scores, indicating areas for further improvement in feature selection.

Despite its strong performance, *FeatNet-IDS* has some limitations. Its FAR is slightly higher compared to the top-performing model [20], and the model is sensitive to hyperparameter tuning. Additionally, there is a potential risk of losing valuable features during dimensionality reduction, which could affect performance in certain scenarios.

In conclusion, *FeatNet-IDS* showcases strong performance and interpretability, making it a suitable choice for various anomaly detection tasks. Future research could address the identified limitations to improve its applicability and reliability in more challenging environments.

VII. Conclusion

This paper introduces the FeatNet-IDS framework for anomaly detection in IIoT systems, focusing on enhancing network traffic security. The framework leverages advanced feature selection and machine learning techniques, achieving high accuracy (92.3%), low False Alarm Rate (2.73%), and

TABLE VI: Comparing *FeatNet-IDS* to previous methods based on six evaluation metrics

Reference	ROC AUC	F1-Score	Precision	Recall	Accuracy	FAR (%)
FeatNet-IDS	0.968	0.915	0.921	0.915	0.923	2.73
Reddy et al., [17]	0.972	0.930	0.940	0.930	0.928	2.50
Hasan et al. [18]	0.960	0.910	0.900	0.920	0.915	3.20
Abbasi et al. [19]	-	0.920	0.910	0.920	0.925	3.10

strong discriminatory power (96.8% ROC AUC), demonstrating its effectiveness in detecting anomalies.

Our results emphasize the importance of robust feature selection and the need for adaptable anomaly detection models in IIoT environments. While the FeatNet-IDS framework shows strong performance, further research is needed to address hyperparameter tuning challenges. Continued refinement of anomaly detection methods is essential to improve the security of IIoT systems.

REFERENCES

[1] W. Alsabbagh and P. Langendörfer, "Security of Programmable Logic Controllers and Related Systems: Today and Tomorrow," IEEE Open Journal of the Industrial Electronics Society, vol. 4, pp. 659-693, 2023, doi: 10.1109/OJIES.2023.3335976.

[2] W. Alsabbagh, C. Kim and P. Langendörfer, "Silent Sabotage: A Stealthy Control Logic Injection in IIoT Systems," 2024 Silicon Valley Cybersecurity Conference (SVCC), Seoul, Korea, Republic of, 2024, pp. 1-8, doi: 10.1109/SVCC61185.2024.10637363.

[3] W. Alsabbagh, S. Amogbonjaye, C. Kim and P. Langendörfer, "Pirates of the MQTT: Raiding IIoT Systems with a Rogue Client," presented at the 8th Cyber Security in Networking Conference (CSNet), 2024, Paris, France, doi: 10.13140/RG.2.2.11963.84004.

[4] W. Alsabbagh, C. Kim and P. Langendörfer, "A Payload of Lies: False Data Injection Attacks on MQTT-based IIoT Systems," presented at 50th Annual Conference of the IEEE Industrial Electronics Society, Chicago, USA, 2024, doi: 10.13140/RG.2.2.14002.58565.

[5] W. Alsabbagh, C. Kim, N. S. Patil and P. Langendörfer, "Beyond the Lens: False Data Injection Attacks on IIoT-Cameras through MQTT Manipulation," 2024 7th Conference on Cloud and Internet of Things (CIoT), Montreal, QC, Canada, 2024, pp. 1-7, doi: 10.1109/CIoT63799.2024.10757025.

[6] W. Alsabbagh, C. Kim, N. S. Patil and P. Langendörfer, "Hacking the Backbone: Shell Reverse Attacks on IIoT Systems," presented at the 21st International Conference on Embedded Wireless Systems and Networks (EWSN), Abu Dhabi, Emirates, 2024, doi: 10.13140/RG.2.2.11963.84004.

[7] U. Hunkeler, H. L. Truong, and A. Stanford-Clark, "MQTT-S—A publish/subscribe protocol for wireless sensor networks," in Proc. IEEE 3rd Int. Conf. Commun. Syst. Softw. Middleware Workshops (COMSWARE), 2008, pp. 791–798.

[8] I. Vaccari, M. Aiello and Enrico Cambiaso, "SlowITe, a Novel Denial of Service Attack Affecting MQTT," in Sensors 2020, 20(10), 2932, doi: 10.3390/s20102932.

[9] Muhammad Husnain et al., "Preventing MQTT Vulnerabilities Using IoT-Enabled Intrusion Detection System," in Sensors 2022, 22(2), 567, doi: 10.3390/s22020567.

[10] M. Thottan and Chuanyi Ji, "Anomaly detection in IP networks," in IEEE Transactions on Signal Processing, vol. 51, no. 8, pp. 2191-2204, Aug. 2003, doi: 10.1109/TSP.2003.814797

[11] M. H. Bhuyan, D. K. Bhattacharyya and J. K. Kalita, "Network Anomaly Detection: Methods, Systems and Tools," in IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 303-336, First Quarter 2014, doi: 10.1109/SURV.2013.052213.00046.

[12] A. H. Hamamoto, L. F. Carvalho, L. D. H. Sampaio, T. Abrão and M. L. Proença, "Network Anomaly Detection System using Genetic Algorithm and Fuzzy Logic," in Expert Systems with Applications, V. 92, pp. 390–402, 2018, doi: 10.1016/j.eswa.2017.09.013.

[13] S. Naseer et al., "Enhanced Network Anomaly Detection Based on Deep Neural Networks," in IEEE Access, vol. 6, pp. 48231-48246, 2018, doi: 10.1109/ACCESS.2018.2863036.

[14] A. Nagaraja, U. Boregowda, K. Khatatneh, R. Vangipuram, R. Nuvvusetty and V. Sravan Kiran, "Similarity Based Feature Transformation for Network Anomaly Detection," in IEEE Access, vol. 8, pp. 39184-39196, 2020, doi: 10.1109/ACCESS.2020.2975716.

[15] M. H. Bhuyan, D. K. Bhattacharyya and J.K. Kalita, "A multi-step outlier-based anomaly detection approach to network-wide traffic," in Information Sciences, v. 348, pp. 243-271, doi: 10.1016/j.ins.2016.02.023.

[16] G. D'angelo, F. Palmieri, M. Ficco and Salvatore Rampone, "An uncertainty-managing batch relevance-based approach to network anomaly detection," in Applied Soft Computing, v. 36: 408–418. ISSN 15684946. doi: 10.1016/j.asoc.2015.07.029.

[17] D. K. Reddy, H. S. Behera, J. Nayak, P. Vijayakumar, B. Naik and P. K. Singh, "Deep neural network based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities," in Transactions on Emerging Telecommunications Technologies, 32(7):e4121, doi: 10.1002/ett.4121.

[18] M. Hasan, M. M. Islam, M. I. I. Zarif and M.M.A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," in Internet of Things, 7:100059, doi: 10.1016/j.iot.2019.100059.

[19] F. Abbasi, M. Naderan and S. E. Alavi, "Anomaly detection in Internet of Things using feature selection and classification based on Logistic Regression and Artificial Neural Network on N-BaIoT dataset," 2021 5th International Conference on Internet of Things and Applications (IoT), Isfahan, Iran, 2021, pp. 1-7, doi: 10.1109/IoT52625.2021.9469605.

[20] K. DeMedeiros, A. Hendawi and M. Alvarez, "A Survey of AI-Based Anomaly Detection in IoT and Sensor Networks, in Sensors 2023, 23(3):1352, doi: 10.3390/s23031352.

[21] A. C. Panchal, V. M. Khadse and P. N. Mahalle, "Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures," 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India, 2018, pp. 124-130, doi: 10.1109/GCWCN.2018.8668630.

[22] D. Serpanos, "Industrial Internet of Things: Trends and Challenges," in Computer, vol. 57, no. 1, pp. 124-128, Jan. 2024, doi: 10.1109/MC.2023.3331552.

[23] A. L. de Sousa and A. S. de Oliveira, "Order-Controlled Production Employing Multi-Agent and Flexible Job-Shop Scheduling on a Physical Simulation Platform," 2022 Latin American Robotics Symposium (LARS), 2022 Brazilian Symposium on Robotics (SBR), and 2022 Workshop on Robotics in Education (WRE), São Bernardo do Campo, Brazil, 2022, pp. 229-234, doi: 10.1109/LARS/SBR/WRE56824.2022.9995868.

[24] B. Sayegh, "FeatNet-IDS," GitHub repository, Available: https://github.com/BahijSayegh/FeatNet-IDS.git.

[25] B. Sayegh, "Dataset,". Available: https://btude-my.sharepoint.com/personal/bahij_sayegh_b-tu_de/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Fbahij%5Fsayegh%5Fb%2Dtu%5Fde%2FDocuments%2FThesis%2FDataset%2FProcessed&ga=1.