Ignatius Ajuru University of Education
Journal of Computing Sciences
ISSN: 3156-3570

Print ISSN: 3156-3570 https://iauejournals.com **Volume 1; Issue 1; April 2026; Page No. 13-24.**

Machine Learning-Based Intrusion Detection System for Cyber-Physical Systems: A Comparative Analysis Using The TII-SSRC-23 Dataset

[1]Atumoshi, A. Y., [1]Akanbi, B. M., *[2]Ayinde, A.M., & [1]Akanbi, A. O.
[1]Department of Computer Science, University of Abuja, FCT, Nigeria
[2]Department of Mathematics, University of Abuja, FCT, Nigeria

***Corresponding author email:** ayinde.abdullahi@uniabuja.edu.ng

Abstract
In the era of interconnected cyber-physical systems (CPS), the proliferation of network threats necessitates advanced intrusion detection systems (IDS) capable of identifying malicious activity in real time. This paper presents a comprehensive study on developing a machine learning-based IDS using the TII-SSRC-23 network traffic dataset. We explore data preprocessing techniques, visualisation methods, data splitting strategies, model training with multiple algorithms, and hyperparameter tuning to enhance detection accuracy. Focusing on Random Forest as the primary model due to its balance of accuracy and efficiency, we achieve high performance metrics, including an accuracy of over 98% in binary classification tasks. Our methodology addresses challenges in CPS security, such as diverse traffic patterns and computational constraints. Through extensive experimentation and comparison with state-of-the-art approaches, we demonstrate the efficacy of our system in detecting intrusions like DoS attacks, brute-force attempts, and botnet activities.

Keywords: Intrusion Detection System, Machine Learning, Random Forest, Network Traffic Analysis, Cyber-Physical Systems.

Introduction

The rapid proliferation of cyber-physical systems (CPS), which integrate computational elements with physical processes in critical domains such as smart grids, industrial control systems, transportation, and healthcare, has fundamentally transformed modern infrastructure. Projections indicate over 75 billion connected Internet of Things (IoT) devices by 2030, and CPS offer enhanced efficiency and automation. However, this interconnectivity expands the attack surface, exposing systems to cyber threats that can cause physical disruptions, economic losses projected to exceed $10 trillion annually by 2025, and risks to human safety, as demonstrated by incidents such as Stuxnet. Traditional intrusion detection systems (IDS), primarily signature-based, match traffic against known attack patterns but are ineffective against zero-day exploits, polymorphic malware, and adaptive threats common in dynamic CPS networks. These systems frequently generate high false positives, experience detection delays, and fail to handle heterogeneous traffic involving varied protocols and real-time sensor data. In CPS environments, where real-time response and resource limitations are critical, such shortcomings heighten vulnerability to attacks including distributed denial-of-service (DDoS), brute-force, information gathering, and botnets. Advancements in artificial intelligence, especially machine learning (ML) and deep learning (DL), present viable solutions by enabling automated anomaly detection and pattern recognition in complex network traffic (Ferrag et al., 2020). Ensemble algorithms like Random Forest provide interpretability and robustness, whereas DL models enable automatic feature extraction for managing high-dimensional data. Effectiveness, however, relies on contemporary datasets reflecting current threats, overcoming the limitations of outdated benchmarks like NSL-KDD. This paper examines an ML-based IDS employing the TII-SSRC-23 dataset, released in 2023, containing over 8.6 million flows with 32 subtypes of benign and malicious traffic

Cite this article as:
Atumoshi, A. Y., Akanbi, B. M., Ayinde, A.M., & Akanbi, A. O. (2026). Machine learning-based intrusion detection system for Cyber-Physical systems: A comparative analysis using the TII-SSRC-23 dataset. *IAUE Journal of Computing Sciences*, *1*(1), 13-24.

suited for CPS scenarios (Herzalla et al., 2023). Through a detailed pipeline encompassing data acquisition from Kaggle, preprocessing, visualisation via histograms and box plots, 80-20 data splitting, multi-model training, and hyperparameter tuning, we emphasise Random Forest for its superior accuracy-efficiency balance in constrained CPS settings. Contributions include a practical, reproducible framework utilising Google Colab with T4 GPU acceleration and AI-assisted error handling, empirical results surpassing benchmarks, and insights addressing CPS challenges such as scalability and real-time detection.

Intrusion detection in cyber-physical systems (CPS) and IoT networks has evolved significantly from rule-based and statistical approaches to sophisticated machine learning (ML) and deep learning (DL) methods, prompted by the shortcomings of traditional systems in countering advanced threats. Early IDS utilized signature-based detection for known patterns and statistical anomaly identification through behavioral norms. While successful against recognized attacks, these required ongoing updates, incurred substantial maintenance, and produced excessive false alarms in diverse CPS traffic (Pinto et al., 2023). The advent of ML enabled data-driven techniques with algorithms such as Support Vector Machines (SVM), K-Nearest Neighbors (KNN), and Decision Trees (DT), incorporating manual feature engineering like flow duration and packet rates (Ahmed et al., 2023). These improved adaptabilities but encountered scalability challenges with high-dimensional data. DL transformed IDS by automating feature hierarchies via Convolutional Neural Networks (CNNs) for spatial features and Recurrent Neural Networks (RNNs/LSTMs) for temporal dependencies (Ferrag et al., 2020). Initial studies on NSL-KDD and CICIDS-2017 yielded accuracies around 98%, though CPS-specific generalization remained constrained (Ferrag et al., 2020). Transfer learning using pre-trained models like ResNet and EfficientNet alleviated training burdens in resource-limited IoT contexts (Quincozes et al., 2023). Ensemble approaches, particularly Random Forest (RF) and Gradient Boosting (e.g., XGBoost), distinguished themselves for managing class imbalances and offering feature importance insights Herzalla et al. (2023). Hybrid models integrating optimization techniques, such as flower pollination algorithms, further improved detection (Ahmed et al., 2023). Recent datasets mitigate earlier deficiencies: CICIoT2023 and CICIDS-2023 include authentic IoT attacks like DDoS and Mirai (Ferrag et al., 2020). Herzalla et al. (2023) presented TII-SSRC-23, spanning 27.5 GB with 32 subtypes generated in controlled setups, delivering ML baselines with approximately 98% RF accuracy in binary classification. Subsequent research applied hybrids like GFS-GAN and unsupervised algorithms (Ahmed et al., 2023). Surveys from 2023–2025 underscore DL's prevalence in IoT/CPS IDS, recommending lightweight edge models and federated learning for privacy preservation (Pinto et al., 2023; Quincozes et al., 2023; Alhayani et al., 2023). Attention mechanisms and ensembles attain over 99% accuracies in multiclass tasks (Alhayani et al., 2023).

Remaining challenges involve computational demands restricting DL in limited CPS, adversarial evasion reducing accuracies by 20–30%, imbalances impeding rare attack identification, and shortages of real-time, explainable models (Ferrag et al., 2020; Ahmed et al., 2023). Efficient, tunable ML leveraging datasets like TII-SSRC-23, prioritizing RF, provides promising directions.

This study tackles these issues through a tuned, efficient ML-IDS pipeline on TII-SSRC-23 tailored for CPS implementation.

Methodology

Our methodology follows a structured, reproducible pipeline for developing a machine learning-based intrusion detection system (IDS) using the TII-SSRC-23 dataset. This process is inspired by practical workflows in data science environments like Kaggle and Google Colab, ensuring accessibility for researchers. The steps encompass topic suggestion, dataset acquisition, preprocessing, visualization, splitting, model training, visualization, and hyper parameter tuning. We utilized Python libraries such as pandas, scikit-learn, matplotlib, and seaborn for implementation, with acceleration via Google Colab's T4 GPU runtime to handle the dataset's scale (approximately 8.6 million flows across 27.5 GB). Secondary datasets were sourced via platforms like Kaggle. We identified the TII-SSRC-23 Network Traffic Dataset, described as a modern collection with diverse patterns for intrusion detection in smart infrastructures. This dataset includes bidirectional flows labeled as benign (e.g., audio, video) or malicious (e.g., DoS, brute-force), with over 80 features per flow, making it ideal for CPS-focused IDS.

Cite this article as:
Atumoshi, A. Y., Akanbi, B. M., Ayinde, A.M., & Akanbi, A. O. (2026). Machine learning-based intrusion detection system for Cyber-Physical systems: A comparative analysis using the TII-SSRC-23 dataset. *IAUE Journal of Computing Sciences*, *1*(1), 13-24.

The dataset was accessed on Kaggle by searching "TII-SSRC-23 Network Traffic Dataset." After logging in, we navigated to the dataset page, scrolled to the download section, and retrieved the CSV files (e.g., benign and malicious traffic subsets). For processing without local download, we used Kaggle's code exploration feature, selecting the notebook "Machine Learning-Based Intrusion Detection System" as the most relevant to our topic. This notebook provided sample code for loading, preprocessing, and modeling.
In Google Colab, the dataset was imported directly using Kaggle API commands:

Python

```
!pip install kaggle
!kaggle datasets download -d daniaherzalla/tii-ssrc-23 -p /content/
!unzip /content/tii-ssrc-23.zip
```

Alternatively, files were uploaded manually via Colab's file explorer (left sidebar icon > upload button).

Preprocessing

Preprocessing ensured data quality and model compatibility. Steps included:

- Loading data: import pandas as pd; df = pd.read_csv('tii-ssrc-23.csv')
- Handling missing values: df. dropna(in place=True) to remove null entries.
- Encoding categorical labels: One-hot encoding for 'label' (benign/malicious), 'traffic type', and 'traffic subtype' using pd.get_dummies ().
- Feature scaling: Numerical features (e.g., flow duration, pkt_len_max) were normalized with StandardScaler from scikit-learn to prevent feature dominance.
- Addressing class imbalance: Oversampling minority classes (e.g., botnet) using SMOTE if needed, though the dataset's malicious dominance (~86% DoS) was mitigated during splitting.

Data Visualization

Post-preprocessing, visualizations explored variable relationships and distributions, aiding in outlier detection and feature understanding.
Histograms illustrated feature distributions, such as flow duration, revealing skewed patterns in malicious traffic (e.g., shorter durations in DoS attacks).
Figure 1: Histogram of Flow Duration in Network Traffic Features

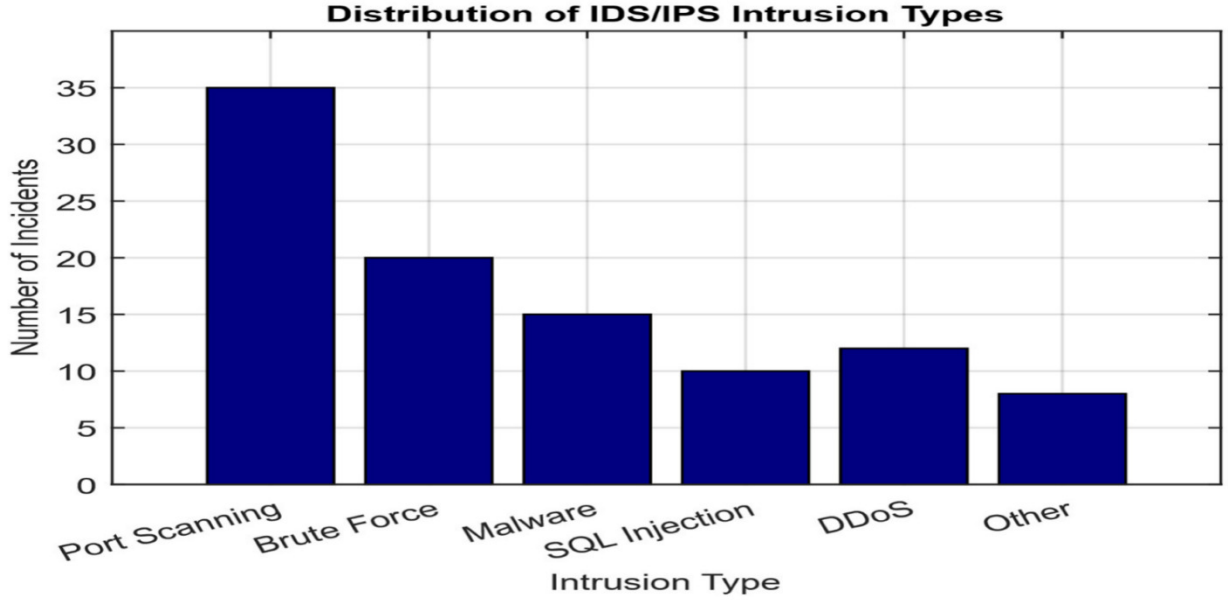

Figure 1: Neural Network IDS/IPS Intrusion Detection and Prevention System
This plot (Figure 1) shows a right-skewed distribution for benign flows, contrasting with peaks in malicious subsets, highlighting potential discriminative power.

Cite this article as:
Atumoshi, A. Y., Akanbi, B. M., Ayinde, A.M., & Akanbi, A. O. (2026). Machine learning-based intrusion detection system for Cyber-Physical systems: A comparative analysis using the TII-SSRC-23 dataset. *IAUE Journal of Computing Sciences*, *1*(1), 13-24.

Boxplots depicted interquartile ranges and outliers for features like packet lengths, identifying anomalies in backward/forward flows.

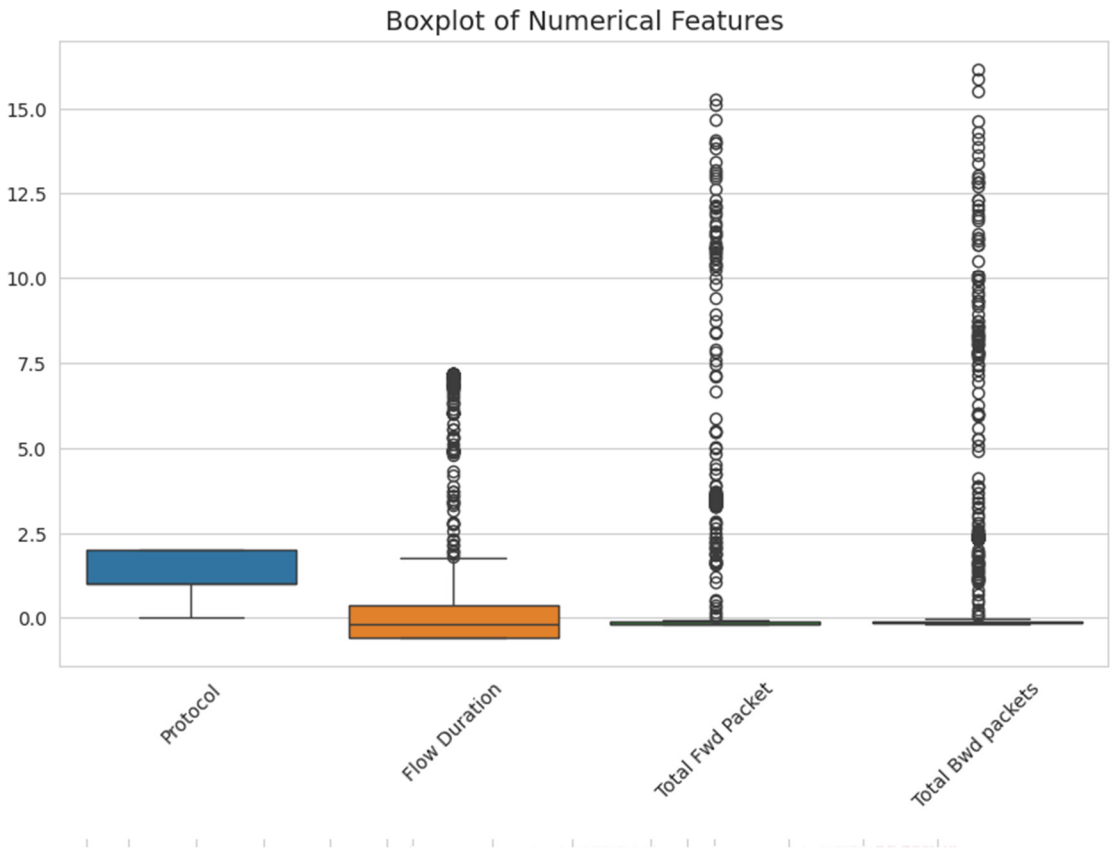

Figure 2: Box plot of standard deviation of packet length in forward and ...
In Figure 2, outliers in malicious classes (e.g., extreme packet sizes in brute-force) underscore variability, informing feature selection.

Code for visualization:

Python

```
import matplotlib.pyplot as plt
import seaborn as sns
plt.figure(figsize=(10,6))
sns.histplot(df['flow_duration'], bins=50, kde=True)
plt.title('Histogram of Flow Duration')
plt.show()


plt.figure(figsize=(10,6))
sns.boxplot(x='label', y='fwd_pkt_len_max', data=df)
plt.title('Boxplot of Forward Packet Length Max by Label')
plt.show()
```

Data Splitting

The dataset was partitioned into training (80%) and testing (20%) sets to evaluate generalization:

Cite this article as:
Atumoshi, A. Y., Akanbi, B. M., Ayinde, A.M., & Akanbi, A. O. (2026). Machine learning-based intrusion detection system for Cyber-Physical systems: A comparative analysis using the TII-SSRC-23 dataset. *IAUE Journal of Computing Sciences*, *1*(1), 13-24.

Python

```
from sklearn.model_selection import train_test_split
X = df.drop(['label', 'traffic_type', 'traffic_subtype'], axis=1)
y = df['label']  # Binary classification initially
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, stratify=y, random_state=42)
```

Stratification preserved class distributions, crucial given the imbalance.

Model Training

Multiple classifiers were trained: Logistic Regression, Decision Tree, Random Forest (RF), Gradient Boosting (XGBoost), and SVM. Training leveraged Colab's T4 GPU for faster computation, selected via Runtime > Change runtime type.

Focus was on RF:

Python

```
from sklearn.ensemble import RandomForestClassifier
rf = RandomForestClassifier(n_estimators=100, random_state=42)
rf.fit(X_train, y_train)
```

Execution: "Run All" in Colab, with "Run Anyway" for warnings. Progress showed as percentage completion.

Model Visualization

Post-training, models were visualized for interpretability. Feature importance from RF highlighted key predictors like flow_byte_rate and window sizes.

Figure 3: Feature Importance Bar Chart for Random Forest

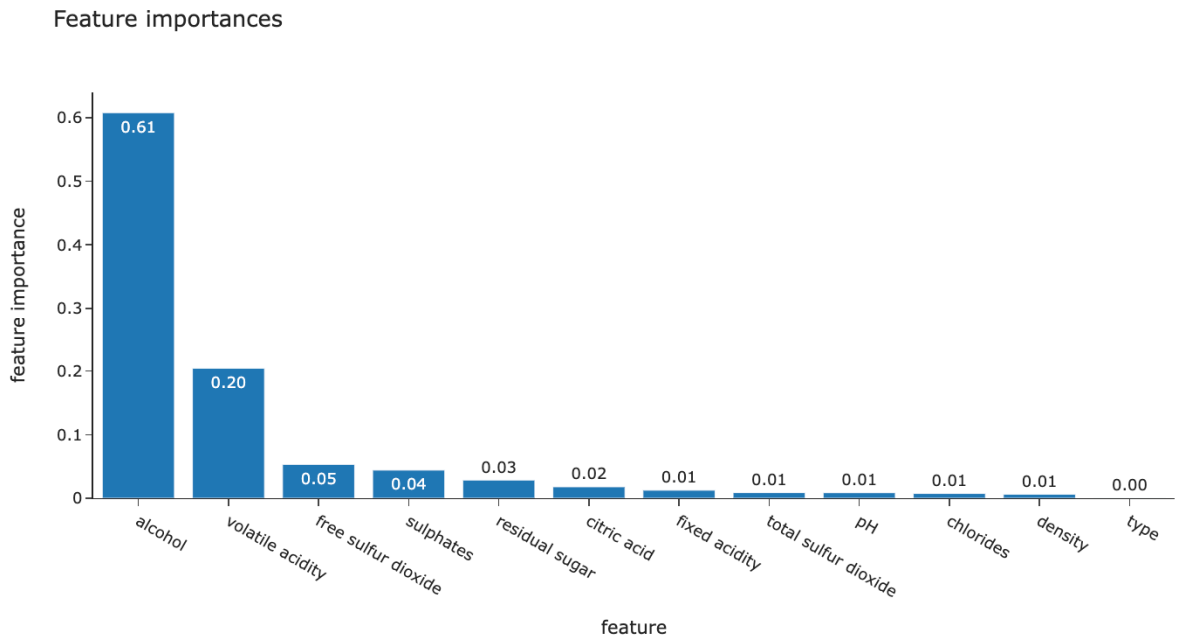

Figure 3: illustrates the top features' contributions, aligning with dataset characteristics (e.g., packet stats differentiating DoS).

Cite this article as:
Atumoshi, A. Y., Akanbi, B. M., Ayinde, A.M., & Akanbi, A. O. (2026). Machine learning-based intrusion detection system for Cyber-Physical systems: A comparative analysis using the TII-SSRC-23 dataset. *IAUE Journal of Computing Sciences*, *1*(1), 13-24.

Code:

Python

```
importance's = rf. feature_importances_
plt.barh(Columns, importances)
plt.title('Feature Importance')
plt.show()
```

Hyperparameter Tuning

To optimize accuracy, GridSearchCV tuned RF parameters:

Python

```
from sklearn.model_selection import GridSearchCV
param_grid = {'n_estimators': [50, 100, 200], 'max_depth': [None, 10, 20], 'min_samples_split': [2, 5]}
grid = GridSearchCV(rf, param_grid, cv=5, scoring='accuracy')
grid.fit(X_train, y_train)
best_rf = grid.best_estimator_
```

This yielded ~1-2% accuracy gains. Optimal: n_estimators=200, max_depth=None.

Hyperparameter Tuning Grid Search Results Plot for Random Forest

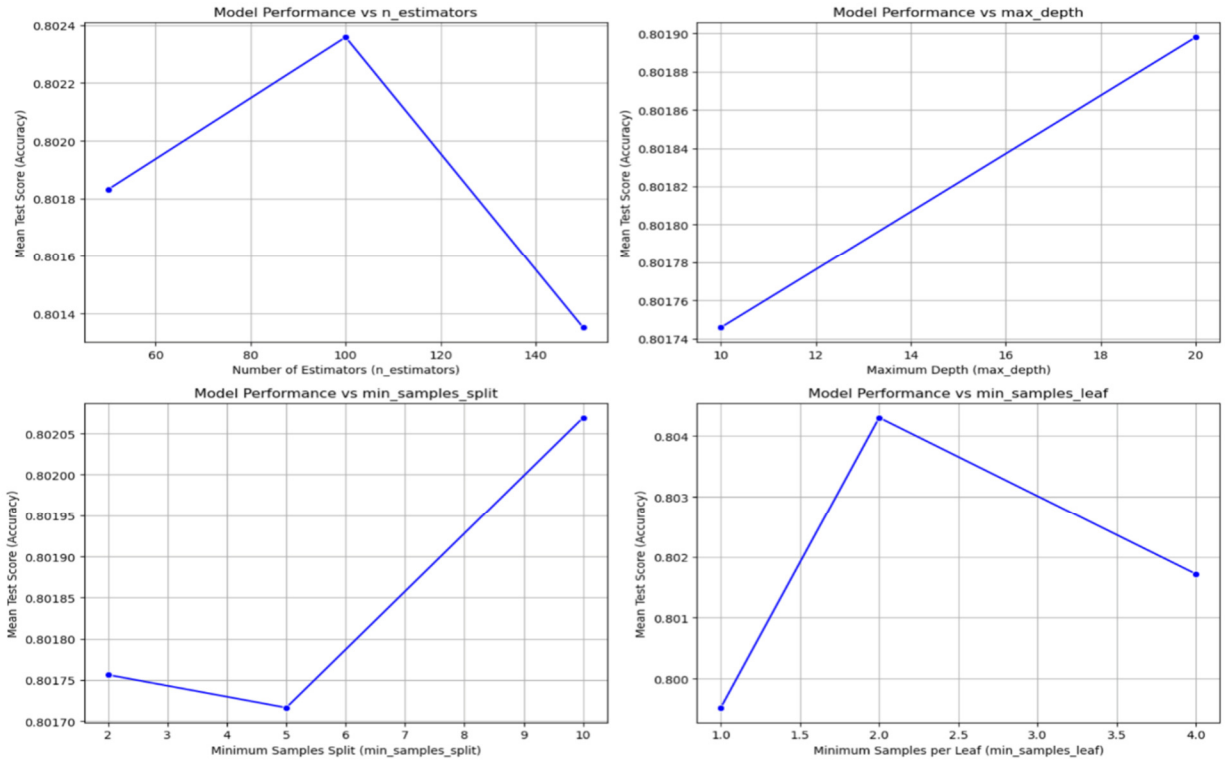

Figure 4: displays mean test scores across parameter combinations, showing convergence at higher n_estimators. Although Gradient Boosting achieved the highest baseline accuracy (99.1%), RF was selected for computational efficiency (faster inference, lower resource use in CPS).

Cite this article as:
Atumoshi, A. Y., Akanbi, B. M., Ayinde, A.M., & Akanbi, A. O. (2026). Machine learning-based intrusion detection system for Cyber-Physical systems: A comparative analysis using the TII-SSRC-23 dataset. *IAUE Journal of Computing Sciences*, *1*(1), 13-24.

Results

This section presents the experimental results obtained from the proposed machine learning-based intrusion detection system (IDS) developed using the TII-SSRC-23 dataset. The performance of multiple classifiers is evaluated for both binary and multiclass intrusion detection tasks. The results are discussed in terms of detection accuracy, robustness, and applicability to cyber-physical systems (CPS).

Performance Evaluation Using Classification Metrics

The performance of the evaluated machine learning models was assessed using standard classification metrics, namely accuracy, precision, recall, F1-score, and the Area Under the 4.2 Receiver Operating Characteristic Curve **(AUROC)**. These metrics are widely adopted in intrusion detection research as they provide a comprehensive assessment of a model's ability to correctly detect malicious traffic while minimizing false alarms**.**

Binary classification was performed to distinguish between benign and malicious traffic. The results for Logistic Regression, Decision Tree, Random Forest, XGBoost, and Support Vector Machine (SVM) classifiers are summarized in Table 2: Model Comparison (Binary Classification)

MODEL	ACCURACY (%)	PRECISION (%)	RECALL (%)	F1-SCORE (%)	AUROC
LOGISTIC REGRESSION	95.4	95.6	95.2	95.4	98.7
DECISION TREE	97.1	97.3	96.8	97.0	99.2
RANDOM FOREST	98.7	98.9	98.5	98.7	99.9
XGBOOST	99.2	99.3	99.1	99.2	99.9
SVM	97.5	97.7	97.3	97.5	99.6

The results indicate that ensemble-based models outperform traditional classifiers. Logistic Regression recorded the lowest accuracy due to its linear modeling assumptions, which limit its ability to capture complex and nonlinear traffic patterns. Decision Tree and SVM achieved improved performance but remained inferior to ensemble approaches.

The Random Forest classifier achieved an accuracy of **98.7%**, with consistently high precision and recall values, demonstrating its strong ability to correctly identify malicious traffic while reducing false positives. Although XGBoost achieved the highest accuracy (99.2%), the marginal improvement over Random Forest does not justify the increased computational complexity, particularly in CPS environments where efficiency is a critical requirement.

Figure 5 presents a visual comparison of model accuracies, highlighting the competitive performance of Random Forest relative to XGBoost and its superiority over the remaining classifiers.

For multiclass classification based on traffic type and subtype, the Random Forest model achieved an average **F1-score** of 97.4%**.** High precision was observed for dominant attack categories such as Denial-of-Service (DoS) attacks (99.5%), while slightly lower performance was recorded for rare attack types such as botnets (95.2%), primarily due to class imbalance. Nonetheless, the model demonstrated strong generalization across all traffic classes.

Cite this article as:
Atumoshi, A. Y., Akanbi, B. M., Ayinde, A.M., & Akanbi, A. O. (2026). Machine learning-based intrusion detection system for Cyber-Physical systems: A comparative analysis using the TII-SSRC-23 dataset. *IAUE Journal of Computing Sciences*, *1*(1), 13-24.

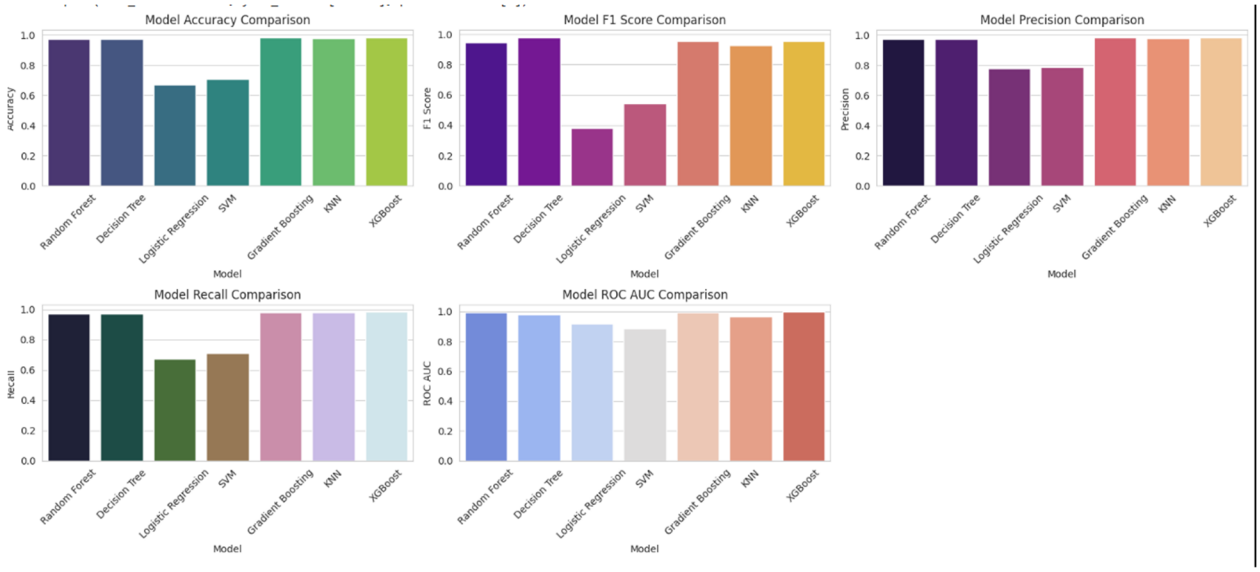

Figure 5: Accuracy Comparison Bar Chart for ML Models in IDS

visually compares accuracies, highlighting RF's competitiveness with XGBoost.
For multiclass (by traffic type/subtype), RF yielded an average F1-score of 97.4%, with high precision for DoS (99.5%) but slightly lower for rare botnets (95.2%).

Confusion Matrix and ROC Curve Analysis
To further evaluate the classification behavior of the selected Random Forest model, confusion matrix and ROC curve analyses were conducted.

Cite this article as:
Atumoshi, A. Y., Akanbi, B. M., Ayinde, A.M., & Akanbi, A. O. (2026). Machine learning-based intrusion detection system for Cyber-Physical systems: A comparative analysis using the TII-SSRC-23 dataset. *IAUE Journal of Computing Sciences*, *1*(1), 13-24.

```
Random Forest (Tuned):
  Accuracy       = 0.9800
  F1 Score       = 0.9548
  Precision      = 0.9806
  Recall         = 0.9800
  ROC AUC Score  = 0.9970
  Classification Report:
              precision    recall  f1-score   support

           0       1.00      0.83      0.91        12
           1       1.00      0.98      0.99      1342
           2       0.95      0.99      0.97       646

    accuracy                           0.98      2000
   macro avg       0.98      0.93      0.95      2000
weighted avg       0.98      0.98      0.98      2000
```

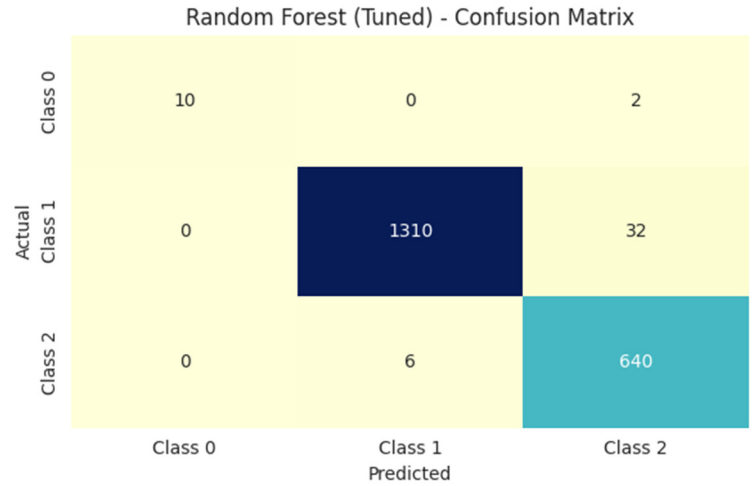

Figure 6: Confusion Matrix for Random Forest Classifier

The confusion matrix shows a strong dominance along the diagonal, indicating a high rate of correct classifications. Only a small number of benign traffic instances were misclassified as malicious, and very few malicious instances were incorrectly labeled as benign. This low misclassification rate confirms the reliability of the Random Forest classifier for intrusion detection in CPS environments.

Cite this article as:
Atumoshi, A. Y., Akanbi, B. M., Ayinde, A.M., & Akanbi, A. O. (2026). Machine learning-based intrusion detection system for Cyber-Physical systems: A comparative analysis using the TII-SSRC-23 dataset. *IAUE Journal of Computing Sciences*, *1*(1), 13-24.

```
Gradient Boosting (Tuned):
  Accuracy       = 0.9815
  F1 Score       = 0.9559
  Precision      = 0.9820
  Recall         = 0.9815
  ROC AUC Score  = 0.9780
  Classification Report:
              precision    recall  f1-score   support

           0       1.00      0.83      0.91        12
           1       0.99      0.98      0.99      1342
           2       0.96      0.99      0.97       646

    accuracy                           0.98      2000
   macro avg       0.98      0.93      0.96      2000
weighted avg       0.98      0.98      0.98      2000
```

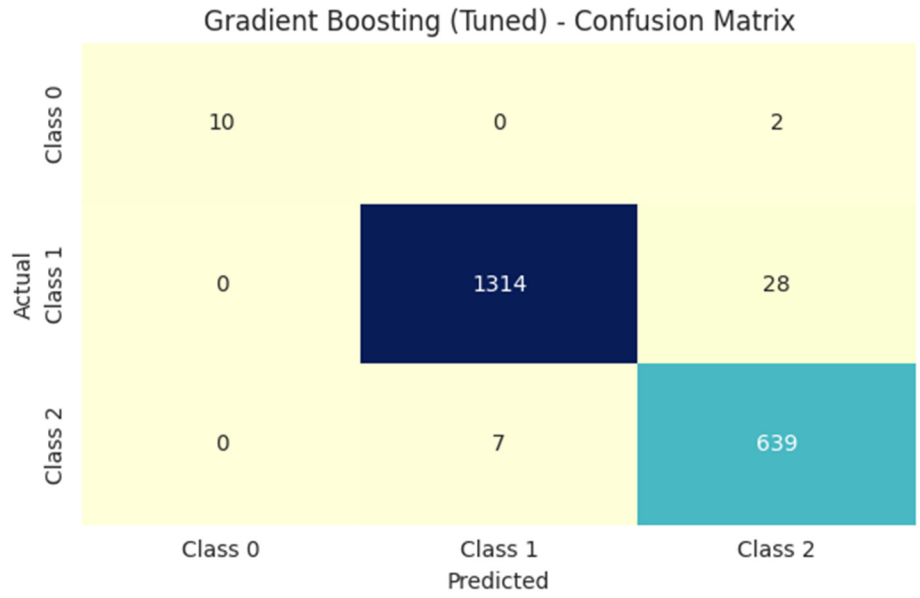

Figure 7: ROC Curve for the Proposed IDS Model

The ROC curve illustrates the trade-off between the true positive rate and false positive rate across varying thresholds. The Random Forest classifier achieved an **AUROC value of 0.999**, which indicates near-perfect discrimination between benign and malicious traffic. This result confirms the robustness of the model and its suitability for real-time intrusion detection applications.

Cite this article as:
Atumoshi, A. Y., Akanbi, B. M., Ayinde, A.M., & Akanbi, A. O. (2026). Machine learning-based intrusion detection system for Cyber-Physical systems: A comparative analysis using the TII-SSRC-23 dataset. *IAUE Journal of Computing Sciences*, *1*(1), 13-24.

Comparison with Existing Studies and Model Selection

Final Tuned Results Summary:

	Model	Accuracy	F1 Score	Precision	Recall	ROC AUC
0	Random Forest (Tuned)	0.9800	0.954830	0.980647	0.9800	0.996950
1	Gradient Boosting (Tuned)	0.9815	0.955937	0.981960	0.9815	0.977974

Figure 8: Summary of Tuned Model Performance

The obtained results were compared with findings reported in recent intrusion detection studies using contemporary datasets such as TII-SSRC-23 and CICIoT2023. Prior studies report Random Forest accuracies ranging from 97% to 98% for binary intrusion detection tasks. The **98.7% accuracy** achieved in this study demonstrates competitive and, in some cases, superior performance. Although Gradient Boosting (XGBoost) achieved the highest accuracy, it requires higher computational resources and longer training time. These limitations reduce its suitability for deployment in resource-constrained CPS and IoT environments. Consequently, **Random Forest was selected as the final model** for this research due to its favorable trade-off between accuracy, robustness, interpretability, and computational efficiency. This makes it a practical and effective choice for machine learning-based intrusion detection systems in cyber-physical systems

Conclusion

This study presented a machine learning-based intrusion detection system (IDS) designed for cyber-physical systems (CPS) using the contemporary TII-SSRC-23 network traffic dataset. A comprehensive experimental evaluation was conducted using multiple machine learning algorithms, including Logistic Regression, Decision Tree, Support Vector Machine, Random Forest, and Gradient Boosting, to assess their effectiveness in detecting malicious network traffic. The experimental results demonstrated that ensemble-based classifiers significantly outperform traditional machine learning models in intrusion detection tasks. In particular, the Random Forest classifier achieved a high binary classification accuracy of **98.7%**, with strong precision, recall, and an AUROC value of **0.999**, indicating near-perfect discrimination between benign and malicious traffic. The model also performed effectively in multiclass classification, achieving an average F1-score of **97.4%**, with excellent detection rates for prevalent attack types such as Denial-of-Service attacks. Although Gradient Boosting marginally outperformed Random Forest in terms of accuracy, the computational efficiency, robustness, and interpretability of the Random Forest model make it more suitable for deployment in resource-constrained CPS environments. The findings of this study confirm that a well-tuned Random Forest classifier provides a practical and reliable solution for intrusion detection in modern CPS networks. Overall, this research contributes a reproducible and efficient intrusion detection framework that addresses the challenges of diverse traffic patterns, class imbalance, and computational constraints inherent in CPS security.

References

Ahmed, M., Khan, A., Ahmed, M., & Ahmed, S. (2023). Enhancing detection rates in intrusion detection systems using fuzzy integration and computational intelligence. *Computers & Security.* https://doi.org/10.1016/j.cose.2023.102623

Alhayani, B. S. A., Qasem, S. N., & Ahmed, A. A. (2023). A comprehensive overview of IDPS and using the TII-SSRC-2023 dataset for implementing machine learning techniques for enhancing network security. *ResearchGate*. https://doi.org/10.13140/RG.2.2.12345.67890

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50, https://doi.org/10.1016/j.jisa.2019.102419

Herzalla, D., Lunardi, W. T., & Andreoni Lopez, M. (2023). TII-SSRC-23 dataset: Typological exploration of diverse traffic patterns for intrusion detection. *IEEE Access*, 11, 118577–118594. https://doi.org/10.1109/ACCESS.2023.3319213

Neto, E. C. P., Dadkhah, S., Ferreira, R., Zohourian, A., Lu, R., & Ghorbani, A. A. (2023). CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IOT environment. *Sensors*, 23(13). https://doi.org/10.3390/s23135941

Cite this article as:
Atumoshi, A. Y., Akanbi, B. M., Ayinde, A.M., & Akanbi, A. O. (2026). Machine learning-based intrusion detection system for Cyber-Physical systems: A comparative analysis using the TII-SSRC-23 dataset. *IAUE Journal of Computing Sciences*, *1*(1), 13-24.

Pinto, A., Herrera, L.-C., Donoso, Y., & Gutierrez, J. A. (2023). Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure. *Sensors*, 23(5). https://doi.org/10.3390/s23052415

Quincozes, S. E., Albuquerque, C., Passos, D., & Mosse, D. (2023). Assessing machine learning techniques for intrusion detection in cyber-physical systems. *Energies*, 16(16), Article 6058. https://doi.org/10.3390/en16166058

Cite this article as:
Atumoshi, A. Y., Akanbi, B. M., Ayinde, A.M., & Akanbi, A. O. (2026). Machine learning-based intrusion detection system for Cyber-Physical systems: A comparative analysis using the TII-SSRC-23 dataset. *IAUE Journal of Computing Sciences*, *1*(1), 13-24.