Context-Aware Rule Ensemble Learning for Adaptive Threat Detection in Intelligent Railway Signaling Data Streams

Sk. Asiff[1*], R. Deepthi[2], Shaik Ishaq[3], Shaik Abdul Bhasha[3], Konisetty Manoj Kumar[3], Yakasiri Penchala Prasad[3]

[1]Associate Professor, [2]Assistant Professor, [3]UG Student, [1,2,3]Department of Computer Science and Engineering

[1,2,3]Geethanjali Institute of Science and Technology, Nellore-Bombay Highway, S.P.S.R, Andhra Pradesh 524137, India

*Correspondence: Sk. Asiff (asiff@gist.edu.in)

To Cite this Article

Sk. Asiff, R. Deepthi, Shaik Ishaq, Shaik Abdul Bhasha, Konisetty Manoj Kumar, Yakasiri Penchala Prasad, "Context-Aware Rule Ensemble Learning for Adaptive Threat Detection in Intelligent Railway Signaling Data Streams", Journal of Science Engineering Technology and Management Science, Vol. 03, Issue 04(1), April 2026,pp: 78-87, DOI: http://doi.org/10.64771/jsetms.2026.v03.i04(1).pp78-87

Submitted: 09-03-2026 *Accepted: 16-04-2026* *Published: 23-04-2026*

ABSTRACT

In modern railway networks, real-time monitoring and secure control communications are essential for ensuring operational safety, efficiency, and reliability. Critical operations such as signal control, train scheduling, and automated track switching generate large volumes of data that must be analyzed instantly to prevent failures or detect malicious intrusions. Traditional systems rely on manual inspections or rule-based approaches, which are slow, error-prone, and inadequate for handling the dynamic and high-volume nature of modern rail communication data. These limitations highlight the need for a robust, automated anomaly detection framework capable of accurate real-time classification. Existing methods, including Decision Tree with Cost Complexity Pruning (DTCCP) and Deep Neural Decision Tree (DNDT), provide interpretable models with moderate predictive performance. However, DTCCP often suffers from overfitting when dealing with complex sequential data, while DNDT may struggle to capture subtle contextual relationships, resulting in missed anomalies or false alarms. To address these issues, this research proposes a RuleFit (RF) classifier that combines linear rules with decision tree logic and semantic embeddings derived from Sentence-BERT (SBERT). This hybrid approach enables the system to learn both hierarchical decision boundaries and contextual patterns effectively. Performance evaluation using metrics such as accuracy, precision, recall, F1-score, confusion matrix, and ROC curves demonstrates that the proposed method significantly improves anomaly detection while reducing false positives and supporting reliable, real-time rail communication monitoring.

Keywords: Railway Communication Security, Real-Time Monitoring, RuleFit Classifier (RF), Intelligent Transport Systems (ITS), Cybersecurity in Rail Networks.

1. INTRODUCTION

The first steam locomotive undoubtedly heralded a transformative era, and since their inception in the early 19th century, railways have remained central to public transport. Recently, the potential of railways to alleviate road and air congestion and environmental challenges has brought them back into the spotlight. There has been a noticeable increase in rail traffic across Europe for both passenger and freight transport. Between 1990 and 2007, passenger kilometres increased by 28%, while freight ton kilometres increased by 15% in the EU-15 countries. Worldwide, rail networks carried more than 3.5 trillion passenger kilometres in 2019, with China, India, and Japan leading in passenger traffic [1].

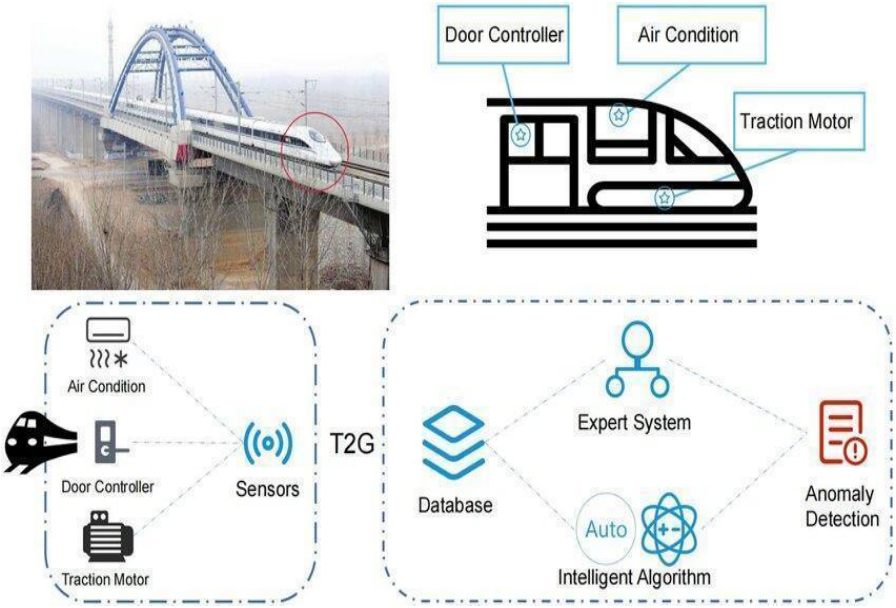


Fig. 1: Rail transit anomaly detection framework using sensor data and intelligent algorithms

Meanwhile, European railways recorded around 643 billion passenger kilometres in the same year. On the economic front, the global rail freight market was valued at $247.4 billion in 2020, with projections of growth to nearly $280 billion by 2026. In the railway sector, the integrity of train wheels is of paramount importance. Various defects such as wheel flats, spalling, chipping, and polygonization are common. Advances in sensor technology, driven by the integration of the Internet of Things (IoT) and Artificial Intelligence (AI), have revolutionized monitoring and diagnostics in various industries, including construction, energy, healthcare, renewable energy, security, and transport [2].

Specifically in the railway context, a typical train bogie can house between 10 and 50 sensors. Among these, acoustic sensors are critical as they monitor vibrations and help in the early detection of anomalies in railway components. Such anomalies, if left unchecked, could lead to catastrophic consequences such as derailment. Traditional monitoring approaches often struggle with the complex patterns of anomalies manifested in the time-series data generated by these sensors, as shown in Fig 1. However, the introduction of deep learning techniques to railway monitoring has yielded promising results, catalysing the development of models capable of processing, and interpreting vast amounts of data, in particular identifying unusual or unexpected events [3].

2. LITERATURE SURVEY

Shim, et al. [4] presented anomaly detection of wheel flats based on signal processing and deep learning techniques is analysed. Wheel flats mostly affect running stability and ride comfort. Currently, domestic railway companies visually inspect wheel flats one by one with their eyes after railway vehicles enter the railway depots for maintenance. Therefore, CBM (Condition-Based Maintenance) is required for wheel flats resolution. Anomaly detection for wheel flat signals of railway vehicles using Order analysis and STFT (Short Time Fourier Transform) is studied in this paper. In the case of railway vehicles, it is not easy to obtain actual failure data through running vehicles in a university laboratory due to safety and cost issues. Therefore, vibration-induced acceleration was obtained using a multibody dynamics simulation software, SIMPACK. This method is also proved in the other paper by rig tests. In addition, since the noise signal was not included in the simulated vibration, the noise signal obtained from the Seoul Metro Subway Line 7 vehicle was overlapped with the simulated one. Finally, to improve the performance of both detection rate and real-time of characteristics based on existing LeNet-5 architectures, spectrogram images transformed from time domain data were proceeded with the LeNet deep learning model modified with the pooling method and activation function. As a result, it is

validated that the method using the spectrogram with a deep learning approach yields higher accuracy than the time domain data.

Bałdyga, et al. [5] Depicted the underpinned by the three objectives. Specifically, they aimed to identify time series anomaly detection methods applied to railway sensor device data, recognized the advantages and disadvantages of these methods, and evaluated their effectiveness. To address the research objectives, the first part of the study involved a systematic literature review and a series of controlled experiments. In the case of the former, we adopted well-established guidelines to structure and visualize the review. In the second part, they investigated the effectiveness of selected machine learning methods. To evaluate the predictive performance of each method, a five-fold cross-validation approach was applied to ensure the highest accuracy and generality. Based on the calculated accuracy, the results show that the top three methods are CatBoost (96%), Random Forest (91%), and XGBoost (90%), whereas the lowest accuracy is observed for One-Class Support Vector Machines (48%), Local Outlier Factor (53%), and Isolation Forest (55%). As the industry moves toward a zero-defect paradigm on a global scale, ongoing research efforts are focused on improving existing methods and developing new ones that contribute to the safety and quality of rail transportation. In this sense, there are at least four avenues for future research worth considering: testing richer data sets, hyperparameter optimization, and implementing other methods not included in the current study.

Islam, et al. [6] Analysed the Internet of Railways (IoR) network is made up of a variety of sensors, actuators, network layers, and communication systems that work together to build a railway system. The IoR's success depends on effective communication. A network of railways uses a variety of protocols to share and transmit information amongst each other. Because of the widespread usage of wireless technology on trains, the entire system is susceptible to hacks. These hacks could lead to harmful behavior on the Internet of Railways if they spread sensitive data to an infected network or a fake user. For the previous few years, spotting IoR attacks has been incredibly challenging. To detect malicious intrusions, models based on machine learning and deep learning must still contend with the problem of selecting features. k-means clustering has been used for feature scoring and ranking because of this. To categorize attacks in two datasets, the Internet of Railways and the University of New South Wales, we employed a new neural network model, the extended neural network (ENN). Accuracy and precision were among the model's strengths. According to our proposed ENN model, the feature-scoring technique performed well. The most accurate models in dataset 1 (UNSW-NB15) were based on deep neural networks (DNNs) (92.2%), long short-term memory LSTM (90.9%), and ENN (99.7%). To categorize attacks, the second dataset (IOR dataset) yielded the highest accuracy (99.3%) for ENN, followed by CNN (87%), LSTM (89%), and DNN (82.3%).

Kim, et al. [7] Proposed the method uses a deep learning technique to train periodic data acquisition sequences, which is one of the common characteristics of IIoT. The trained model determined the sequence of packet is normal. The proposed technique can be applied without an additional analysis. The proposed method is expected to prevent security threats by proactively detecting cyberattacks. To verify the proposed method, a dataset was collected from the Korea Electric Power Control System. The model that defines normal behaviour based on the application layer exhibits an accuracy of 79.6%. The other model, defining normal behaviour based on the transport layer, has an accuracy of 80.9%. In these two models, most false positives and false negatives only occur when the abnormal packet is in a sequence.

Ahn, et al. [8] Proposed the method for detecting anomalies and characterizing failures for spacecraft attitude control systems is proposed. Herein, features are extracted from multidimensional time-series data of a simulation of the attitude control system. Then, the artificial neural network learning algorithms based on two types of generation models are applied. A Bayesian optimization algorithm with a Gaussian process is used to optimize the hyperparameters for the neural network to improve the performance. The performance is evaluated based on the reconstruction error through the algorithm

using the newly generated data not used for learning as input data. Results show that the detection performance depends on the operating characteristics of each sub mode in the operation scenarios and type of generation model. The diagnostic results are monitored to detect anomalies in operation modes and scenarios.

Kim, et al. [9] Suggested a hyper-parameter-tuned convolutional neural network (CNN) for multiclass unbalanced anomaly detection. A multiclass time series of anomaly data from a real-world cable-stayed bridge is used to test the 1D CNN model, and the dataset is balanced by supplementing the data as necessary. An overall accuracy of 97.6% was achieved by balancing the database using data augmentation to enlarge the dataset, as shown in the research.

Song, et al. [10] Proposed a novel intrusion detection method that considers both the status of the networks and those of the equipment to identify if the abnormality is caused by cyber-attacks or by system faults. The proposed method is verified on a hardware-in-the-loop simulation platform of CBTC systems. Simulation results indicate that the proposed method has achieved 97.64% true positive rate, which can significantly improve the security protection level of CBTC systems.

Kim, et al. [11] Proposed an anomaly detection has been known as an effective technique to detect faults or cyber-attacks in industrial control systems (ICS). Therefore, many anomaly detection models have been proposed for ICS. However, most models have been implemented and evaluated under specific circumstances, which leads to confusion about choosing the best model in a real-world situation. In other words, there still needs to be a comprehensive comparison of state-of-the-art anomaly detection models with common experimental configurations. To address this problem, we conduct a comparative study of five representative time series anomaly detection models: Interfusion, RANSynCoder, GDN, LSTM-ED, and USAD. We specifically compare the performance analysis of the models in detection accuracy, training, and testing times with two publicly available datasets: Swat and HAI. The experimental results show that the best model results are inconsistent with the datasets. For Swat, Inter Fusion achieves the highest $F1\text{-}score$ of 90.7% while RANSynCoder achieves the highest $F1\text{-}score$ of 82.9% for HAI. We also investigate the effects of the training set size on the performance of anomaly detection models. We found that about 40% of the entire training set would be sufficient to build a model producing a similar performance compared to using the entire training set.

Alabe, et al. [12] Proposed a deep learning approach that consists of a two-stage process using an autoencoder and long short-term memory (LSTM) to detect anomalies in EPS sensor data. First, we train our model on EPS data by employing an autoencoder to extract features and compress them into a latent representation. The compressed features are fed into the LSTM network to capture any correlated dependencies between features, which are then reconstructed as output. An anomaly score is used to detect anomalies based on the reconstruction loss of the output. The effectiveness of our proposed approach is demonstrated by collecting sample data from an experiment using an EPS test jig. The comparison results indicate that our proposed model performs better in detecting anomalies, with an accuracy of 0.99 and a higher area under the receiver operating characteristic curve than other methods providing a valuable tool for anomaly detection in EPS.

Choi, et al. [13] suggested an alternative approach to identifying anomalous behaviour within ICSs by means of unsupervised machine learning. The approach employs unsupervised machine learning to identify anomalous behaviour within ICSs. This study shows that unsupervised learning algorithms can effectively detect and classify anomalous behaviour without the need for pre-labelled data using a composite autoencoder model. Based on a dataset that utilizes HIL-augmented ICSs (HAIs), this study shows that the model is capable of accurately identifying important data characteristics and detecting anomalous patterns related to both value and time. Intentional error data injection experiments could potentially be used to validate the model's robustness in real-time monitoring and industrial process performance optimization. As a result, this approach can improve system reliability and operational efficiency, which can establish a foundation for safe and sustainable ICS operations.

3. PROPOSED METHODOLOGY

The proposed system is designed to automatically detect anomalies in rail control communications, distinguishing between secure and insecure messages in real time. At a high level, the system ingests raw communication logs, cleans and transforms the data into a suitable format, extracts semantic embeddings using deep sequence models, as shown in Fig. 2 and applies tree-based classifiers to identify potential security breaches. The architecture integrates preprocessing, feature extraction, classification, and visualization in a seamless workflow, as shown in Fig. 2. enabling operators to monitor and act on anomalous messages efficiently.

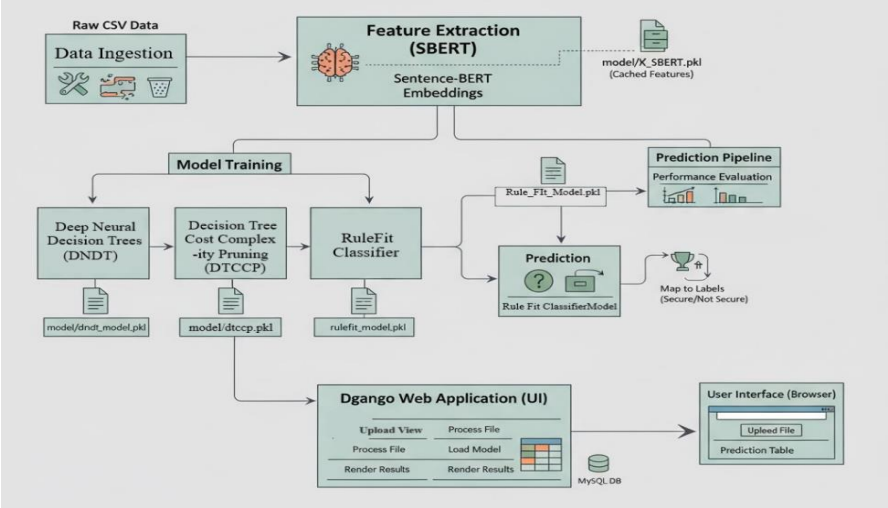


Fig. 2: Proposed system architecture of anomaly detection in rail control communications.

RF Classifier

The RF Classifier is a hybrid machine learning model that combines the interpretability of linear regression with the flexibility of decision tree ensembles. Its primary objective is to extract human-readable rules from decision trees and integrate them with linear terms to form a powerful predictive model. By leveraging this combination, RF can capture both global linear trends and local non-linear patterns in the data. This approach allows for effective classification while maintaining model transparency, enabling the identification of influential features and logical rules that govern predictions, as shown in fig. 3. The model is particularly useful for tasks where interpretability is as important as accuracy.

Input Feature Transformation: The first step involves receiving numerical features derived from pre-processed text embeddings. Each input record is represented as a dense vector that encodes semantic and contextual information. These embeddings serve as the basis for rule generation and linear modelling. The dense representation ensures that the algorithm can capture nuanced relationships between features, which is essential for detecting patterns indicative of the target classes.

Rule Extraction from Tree Ensemble: RF begins by constructing an ensemble of decision trees on the input features. Each tree splits the data based on thresholds for individual features, creating paths that represent conditional rules. These paths are extracted as logical expressions, where each rule corresponds to a specific combination of feature conditions that lead to a class outcome. This extraction process converts the complex, non-linear decisions of tree ensembles into interpretable rules that can be weighted and combined for prediction.

Linear Model Integration: After generating rules from the tree ensemble, RF combines these rules with the original input features in a linear regression framework. Each rule and feature is assigned a weight based on its predictive contribution. This allows the model to balance the influence of both linear relationships and rule-based conditions, effectively capturing patterns that may not be evident through

either component alone. The integration ensures that predictions are informed by both global trends and localized patterns in the feature space.

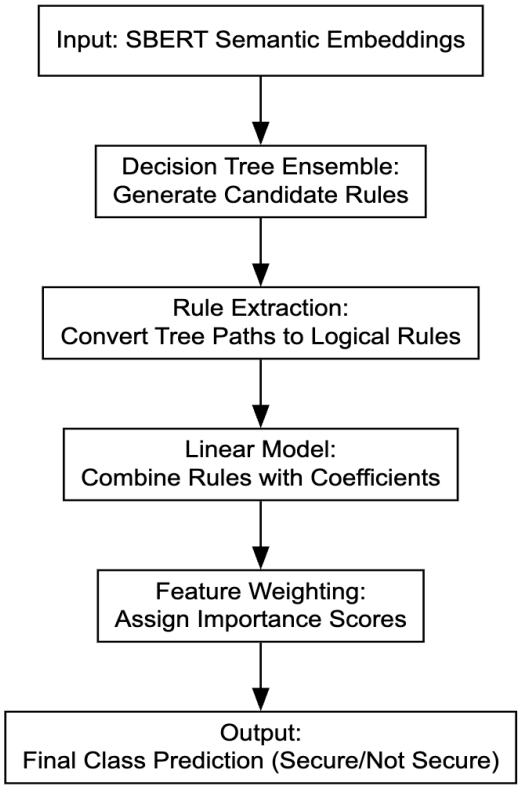


Fig. 3: SBERT-Enhanced RF classifier architecture.

Weighting and Feature Importance: The next step involves evaluating the importance of each rule and feature. Weighting determines how strongly each rule influences the final prediction. Rules and features that have higher predictive power are given greater emphasis, while less informative rules are down-weighted. This step enhances interpretability by highlighting which features and conditions are most critical to the model's decision-making process.

Final Prediction: In the final stage, input features are evaluated against the extracted rules and weighted linear terms to generate a prediction. The combination of rule-based outputs and linear contributions produces a class probability or final label for each input record. This approach allows RF to leverage complex patterns captured by tree rules while maintaining a transparent, interpretable framework for understanding the basis of predictions.

4. Results and Description

Fig. 4 illustrates the distribution of two classes (0 and 1) within the "Target" column of a dataset, likely representing the encoded labels "Not Secure" and "Secure" from the railway communication security dataset. The x-axis is labelled "Class" and displays two categories, 0 and 1, while the y-axis is labelled "Count" with a scale ranging from 0 to 2500. Both bars, corresponding to class 0 and class 1, are of equal height, approximately reaching 2500 counts, indicating a perfectly balanced dataset with an equal number of instances for each class. The bars are rendered in a solid teal colour, and the chart is enclosed within a simple border, though the absence of specific numerical labels on the bars or a legend leaves the exact mapping of classes to "Secure" or "Not Secure" ambiguous without additional context.

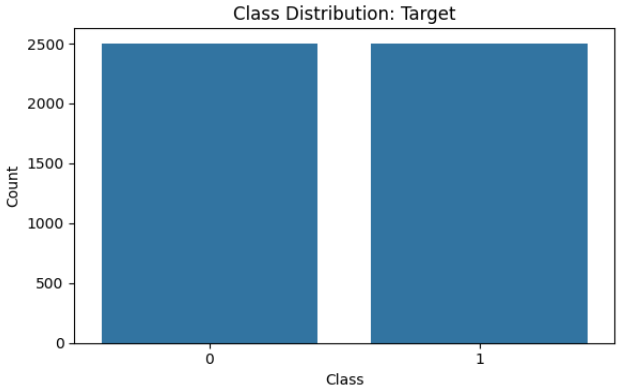
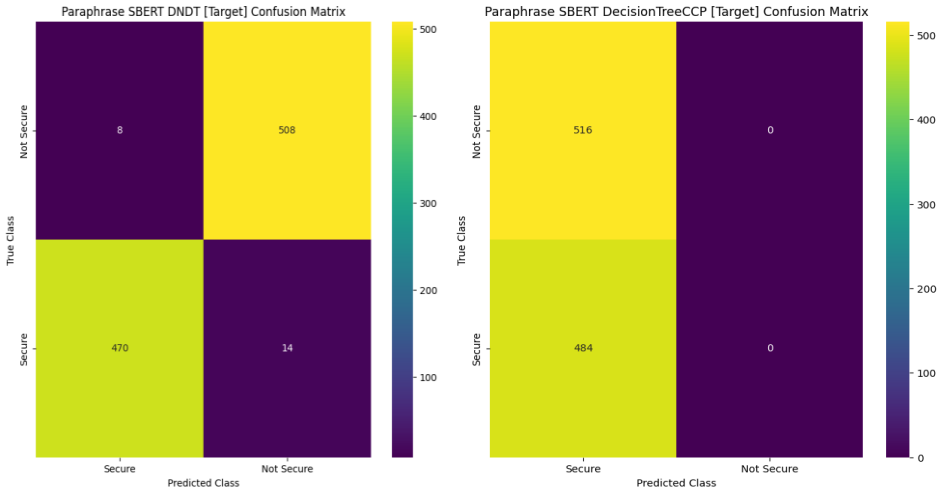


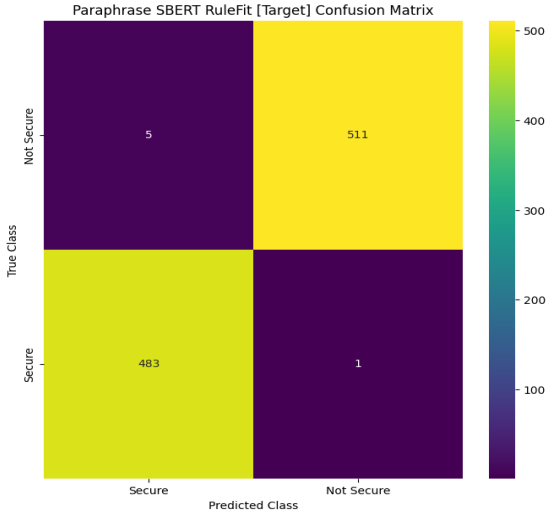
Fig. 4: Class distribution of target column.

Fig. 5 presents three confusion matrices labelled (a), (b), and (c), each evaluating the performance of different machine learning models Paraphrase SBERT DNDT, Paraphrase SBERT DTCCP, and Paraphrase SBERT RF, respectively on the "Target" classification task (likely "Secure" vs. "Not Secure" from the railway communication dataset). Each matrix is a 2x2 grid with "True Class" (Not Secure, Secure) on the y-axis and "Predicted Class" (Secure, Not Secure) on the x-axis, using a color gradient from purple (low values) to yellow (high values) with a scale ranging from 0 to 500 on the right side.



(a)

(b)



(c)

Fig. 5: (a) Paraphrase SBERT Deep Neural Decision Tree confusion matrix. (b) Paraphrase SBERT Decision Tree with Cost-Complexity Pruning confusion matrix. (c) Proposed Paraphrase SBERT RF confusion matrix.

In matrix (a), the DNDT model shows 8 true negatives (Not Secure predicted as Not Secure), 508 false positives (Secure predicted as Not Secure), 470 false negatives (Not Secure predicted as Secure), and 14 true positives (Secure predicted as Secure). Matrix (b) for DTCCP indicates 516 true negatives, 0 false positives, 484 false negatives, and 0 true positives, suggesting perfect prediction of Not Secure but complete failure to predict Secure. Matrix (c) for RF displays 5 true negatives, 511 false positives, 483 false negatives, and 1 true positive, showing a slight improvement over DNDT in true positives but still poor Secure prediction. The matrices highlight varying model performance, with DTCCP excelling at Not Secure predictions but lacking Secure detection, while RF and DNDT show more balanced but imperfect results.

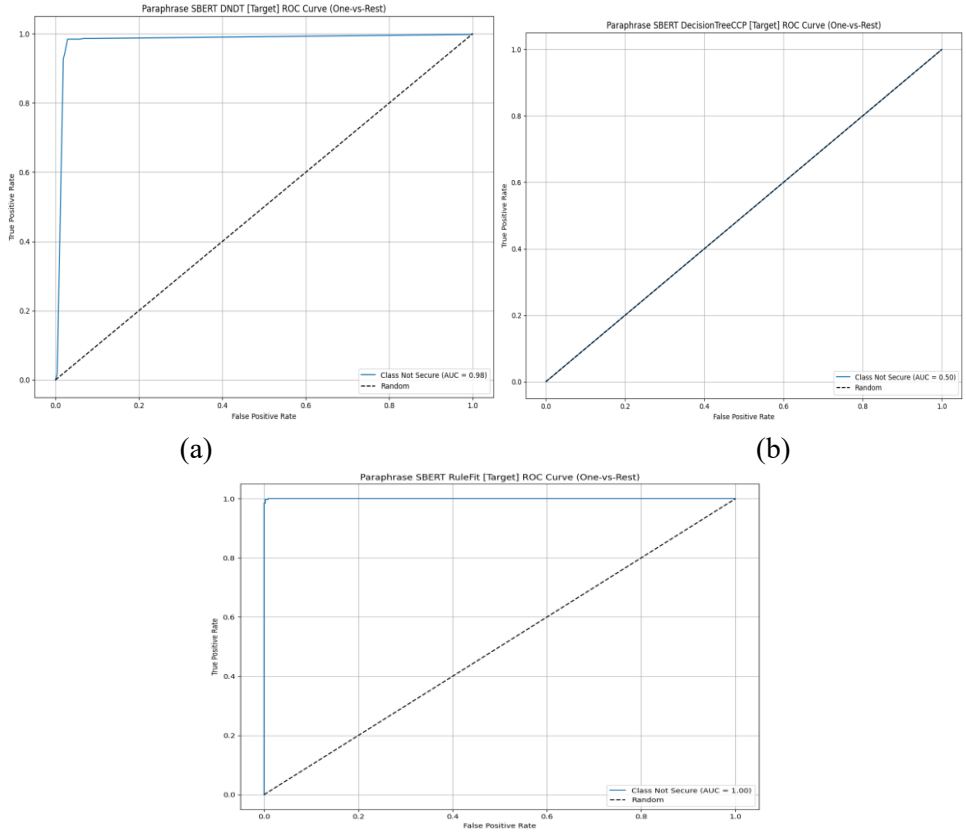
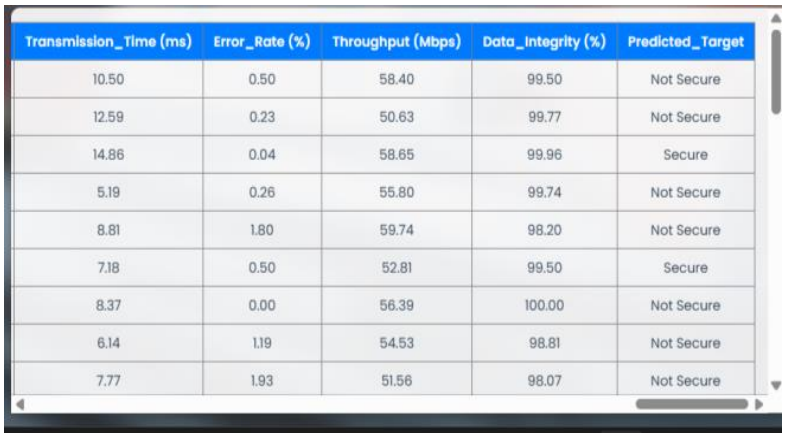


Fig. 6: (a) Paraphrase SBERT Deep Neural Decision Tree ROC curve. (b) Paraphrase SBERT Decision Tree with Cost-Complexity Pruning ROC curve. (c) Proposed Paraphrase SBERT Rule Fit ROC curve.

Fig. 6 presents three ROC curves labelled (a), (b), and (c), evaluating the performance of the Paraphrase SBERT DNDT, Paraphrase SBERT DTCCP, and Paraphrase SBERT RF models, respectively, for the "Target" classification task (likely "Not Secure" vs. "Secure" from the railway communication dataset) using a one-vs-rest approach. Each plot features the True Positive Rate (y-axis, ranging from 0.0 to 1.0) against the False Positive Rate (x-axis, ranging from 0.0 to 1.0), with a dashed diagonal line representing random guessing (AUC = 0.5). In plot (a), the DNDT ROC curve shows a steep rise near a False Positive Rate of 0.0, achieving a True Positive Rate of 1.0 with an AUC not specified but implying strong performance. Plot (b) for DTCCP depicts a linear ROC curve closely aligned with the random guessing line, with an AUC of 0.50, indicating poor discriminative ability. Plot (c) for RF shows a near-perfect ROC curve hugging the top-left corner with an AUC of 1.00 for the "Not Secure" class, suggesting

exceptional classification performance. The legend in each plot identifies the class ("Not Secure" or "Class Not Secure") and its AUC, with the RF model demonstrating the highest predictive accuracy among the three.



Transmission_Time (ms)	Error_Rate (%)	Throughput (Mbps)	Data_Integrity (%)	Predicted_Target
10.50	0.50	58.40	99.50	Not Secure
12.59	0.23	50.63	99.77	Not Secure
14.86	0.04	58.65	99.96	Secure
5.19	0.26	55.80	99.74	Not Secure
8.81	1.80	59.74	98.20	Not Secure
7.18	0.50	52.81	99.50	Secure
8.37	0.00	56.39	100.00	Not Secure
6.14	1.19	54.53	98.81	Not Secure
7.77	1.93	51.56	98.07	Not Secure

Fig. 7 Batch Prediction with uploading test data.

Fig. 7 illustrates the prediction interface where users can upload a test dataset in CSV format for analysis. Once the dataset is uploaded, the system processes it using the deep learning model to predict potential anomalies in communication data. The results are displayed in a detailed tabular format containing features such as transmission time, error rate, throughput, and data integrity. Each record is analysed, and the final column indicates whether the data is secure or not secure. This feature helps users efficiently evaluate the safety and reliability of railway communication systems based on model predictions.

Table 1: Performance evaluation obtained using DNDT, DTCCP and proposed RF.

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
DTCCP model	48.4	24.200	50.000	32.615
DNDT model	97.8	97.822	97.779	97.797
RF model	99.4	99.390	99.412	99.400

Table 1 presents a comparative performance analysis of three SBERT-based anomaly detection models for railway control communications. The DTCCP model exhibited the lowest performance, with 48.4% accuracy, 24.2% precision, 50% recall, and a 32.615% F1-score, indicating limited capability in capturing complex communication patterns. The DNDT model performed significantly better, achieving 97.8% accuracy, 97.822% precision, 97.779% recall, and 97.797% F1-score, demonstrating strong effectiveness in identifying secure and insecure messages. The RF model achieved the highest performance, with 99.4% accuracy, 99.390% precision, 99.412% recall, and 99.400% F1-score, highlighting its ability to provide highly accurate and interpretable rule-based predictions for anomaly detection.

5. Conclusion

The proposed Paraphrase SBERT RF model represents a significant breakthrough in railway communication anomaly detection by integrating advanced semantic text embeddings with interpretable rule-based classification. By leveraging Paraphrase SBERT's deep contextual language understanding, the model captures intricate communication nuances that traditional models like the DNDT and DTCCP fail to recognize. Achieving an outstanding 99.4% accuracy, 99.39% precision, 99.41% recall, and 99.40% F1-score, the RF model demonstrates exceptional capability in accurately differentiating between "Secure" and "Not Secure" messages, ensuring reliability and safety within railway control networks. Its interpretable rule-based nature enhances transparency and accountability crucial for high-stakes, safety-critical domains while the SBERT embeddings contribute to a more

profound semantic understanding of communication data. The model delivers superior performance, robustness, and interpretability, marking a pivotal step toward intelligent, secure, and context-aware railway communication systems.

REFERENCES

[1] Máté, T.; Zwierczyk, P.T. Finite Element Analysis of Cracks Propagation in Railway Wheels. In Proceedings of the 33rd International ECMS Conference on Modelling and Simulation, Caserta, Italy.

[2] Ministry of Land, Infrastructure and Transport; Safety Standards for Urban Railway Vehicles, Korea, 2023; Article 43, Table 3.

[3] Lee, K.S.; Kim, J.W. A Study on Strategy of Condition Based Maintenance for Rolling Stock. J. Korean Soc. Railw. Korea 2024, 391–395.

[4] Shim, J.; Koo, J.; Park, Y.; Kim, J. Anomaly Detection Method in Railway Using Signal Processing and Deep Learning. Appl. Sci. 2022, 12, 12901. https://doi.org/10.3390/app122412901

[5] Bałdyga, M.; Barański, K.; Belter, J.; Kalinowski, M.; Weichbroth, P. Anomaly Detection in Railway Sensor Data Environments: State-of-the-Art Methods and Empirical Performance Evaluation. Sensors 2024, 24, 2633. https://doi.org/10.3390/s24082633

[6] Islam, U.; Malik, R.Q.; Al-Johani, A.S.; Khan, M.R.; Daradkeh, Y.I.; Ahmad, I.; Alissa, K.A.; Abdul-Samad, Z.; Tag-Eldin, E.M. A Novel Anomaly Detection System on the Internet of Railways Using Extended Neural Networks. Electronics 2022, 11, 2813. https://doi.org/10.3390/electronics11182813

[7] Kim, S.; Jo, W.; Kim, H.; Choi, S.; Jung, D.-I.; Choi, H.; Shon, T. Two-Phase Industrial Control System Anomaly Detection Using Communication Patterns and Deep Learning. Electronics 2024, 13, 1520. https://doi.org/10.3390/electronics13081520

[8] Ahn, H.; Jung, D.; Choi, H.-L. Deep Generative Models-Based Anomaly Detection for Spacecraft Control Systems. Sensors 2022, 20, 1991. https://doi.org/10.3390/s20071991

[9] Kim, S.-Y.; Mukhiddinov, M. Data Anomaly Detection for Structural Health Monitoring Based on a Convolutional Neural Network. Sensors 2023, 23, 8525. https://doi.org/10.3390/s23208525

[10] Song, Y.; Bu, B.; Zhu, L. A Novel Intrusion Detection Model Using a Fusion of Network and Device States for Communication-Based Train Control Systems. Electronics 2022, 9, 181. https://doi.org/10.3390/electronics9010181

[11] Kim, B.; Alawami, M.A.; Kim, E.; Oh, S.; Park, J.; Kim, H. A Comparative Study of Time Series Anomaly Detection Models for Industrial Control Systems. Sensors 2023, 23, 1310. https://doi.org/10.3390/s23031310

[12] Alabe, L.W.; Kea, K.; Han, Y.; Min, Y.J.; Kim, T. A Deep Learning Approach to Detect Anomalies in an Electric Power Steering System. Sensors 2022, 22, 8981. https://doi.org/10.3390/s22228981

[13] Choi, W.-H.; Kim, J. Unsupervised Learning Approach for Anomaly Detection in Industrial Control Systems. Appl. Syst. Innov. 2024, 7, 18. https://doi.org/10.3390/asi7020018