AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2) (2026)

Intelligent Detection of Communication Anomalies in Railway Systems Using Deep Sequential Modeling Paradigms

K. Mounika[1], Middinti Deepika[1], Akula Jaya Sree[1], Pasula Bhaskar[1], Karangula Nikhil[1]

[1]Department of Computer Science and Engineering, [1]Sree Dattha Institute of Engineering and Science, Nagarjuna Sagar Road, Sheriguda, Ibrahimpatnam, Rangareddy Dist, 501510, Telangana, India.

ABSTRACT

The growing dependence on digital communication systems in railway infrastructure has created a critical need for intelligent methods to ensure communication security and operational reliability. Railway communication data, including logs, alerts, and textual messages, is highly unstructured and contains valuable indicators of system status, making accurate classification a challenging task due to contextual ambiguity and linguistic variability. The problem addressed in this work is the development of an automated system capable of classifying communication data based on the target column which represents two classes: Secure and Not Secure. The traditional system relies entirely on manual analysis, where experts interpret communication data based on experience, which is time-consuming, inconsistent, error-prone, and not scalable for large datasets. These limitations highlight the need for an efficient automated solution. To address this, the proposed system integrates semantic embedding techniques with interpretable machine learning (ML) models. Text data is transformed into dense vector representations using Sentence Bidirectional Encoder Representations from Transformers (Sentence-BERT or SBERT) based on the Multi-Purpose Encoder Network (MPNet) architecture, enabling effective capture of contextual and semantic information. These embeddings are used to train multiple classifiers, including Differentiable Neural Decision Trees (DNDT), Decision Tree with Cost Complexity Pruning (Decision Tree CCP), and RuleFit, where RuleFit is selected as the final model due to its ability to combine rule-based reasoning with linear modeling. The proposed system ensures accurate, scalable, and interpretable predictions, thereby enhancing railway communication security monitoring and supporting faster, reliable decision-making in critical environments.

Key words: Railway Communication Security, Semantic Embeddings, Natural Language Processing (NLP), Text Classification, Cybersecurity Monitoring, Django Framework.

1. INTRODUCTION

Rail transportation, which began with the introduction of early steam-driven locomotives in the nineteenth century, has developed into a fundamental component of global mobility systems. In recent decades, railways have regained prominence due to their capacity to offer energy-efficient, cost-effective, and environmentally sustainable transportation compared to road and air travel. The growth in rail usage is particularly evident across Europe, where both passenger and freight movement have steadily increased over time. Statistical trends indicate a significant rise in passenger travel and freight operations across EU-15 countries, reflecting the expanding reliance on rail infrastructure. Globally, railway networks facilitated more than 3.5 trillion passenger kilometres in 2019, with major contributions from densely populated nations such as China, India, and Japan, highlighting the scale and importance of modern rail systems [1].

In addition to passenger transport, the freight sector has demonstrated substantial economic significance, with the global rail freight market valued in the hundreds of billions and projected to grow further in the coming years. Within this context, maintaining the structural health and operational efficiency of railway components is essential. Train wheels, in particular, are highly susceptible to

defects such as flats, spalling, chipping, and polygonal wear, all of which can adversely affect safety and performance if left undetected. The rapid advancement of sensing technologies, along with the integration of Internet of Things (IoT) and Artificial Intelligence (AI), has significantly enhanced monitoring and diagnostic capabilities across railway systems [2].

Modern railway bogies are typically equipped with multiple sensors, often ranging between 10 and 50, to continuously monitor operational conditions. Among these, acoustic and vibration sensors play a critical role in capturing patterns associated with mechanical behavior, enabling early identification of potential faults. If such anomalies are not detected at an early stage, they may escalate into severe incidents, including derailments and major system failures. Conventional monitoring approaches, which rely heavily on manual inspection or basic analytical techniques, often struggle to interpret the complex and nonlinear characteristics of time-series sensor data. In contrast, deep learning-based approaches have shown strong potential in effectively analyzing large-scale data and identifying subtle anomalies with higher accuracy [3].

Despite the availability of various anomaly detection techniques, there remains a need for comprehensive evaluation strategies that combine both qualitative understanding and quantitative validation [4]. Many existing studies focus on isolated aspects, either reviewing methods or presenting experimental results, without integrating both perspectives. Therefore, there is a growing demand for research that systematically examines existing approaches while validating their performance on real-world datasets. Addressing this gap is crucial for developing robust and adaptive monitoring systems, and this work contributes by combining analytical review with empirical evaluation to enhance railway fault detection methodologies [5].

2. LITERATURE SURVEY

Shim, et al. [6] proposed a comprehensive anomaly detection framework for identifying wheel flat defects in railway systems by integrating advanced signal processing techniques with deep learning. Since acquiring real-world faulty data is difficult due to safety and cost constraints, vibration-induced acceleration signals were generated using SIMPACK simulation software and combined with real noise data collected from operational railway systems. The study applied Order Analysis and Short Time Fourier Transform (STFT) to convert time-domain signals into spectrogram representations, which were then processed using a modified LeNet-5 architecture with improved pooling and activation functions. The results demonstrated that spectrogram-based deep learning approaches provide higher accuracy and robustness compared to traditional time-domain analysis. Bałdyga, et al. [7] conducted an extensive study that combined systematic literature review with experimental validation to analyze anomaly detection techniques for railway sensor data. The research focused on identifying effective time-series detection methods and evaluating their performance using a five-fold cross-validation approach. The results showed that CatBoost achieved the highest accuracy of 96%, followed by Random Forest (91%) and XGBoost (90%), while methods such as One-Class Support Vector Machine, Local Outlier Factor, and Isolation Forest exhibited lower performance. The study emphasized the importance of high-quality datasets, proper model selection, and hyperparameter optimization.

Islam, et al. [8] addressed security challenges in the Internet of Railways (IoR), where interconnected communication systems are vulnerable to cyber threats. The authors proposed an Extended Neural Network (ENN) combined with k-means clustering for feature selection and ranking, enabling efficient handling of high-dimensional data. The model was evaluated on benchmark datasets such as UNSW-NB15 and IoR datasets, achieving accuracy up to 99.7% and 99.3%, respectively. The results demonstrated that the proposed model outperformed conventional deep learning approaches like CNN and LSTM in intrusion detection tasks. Kim, et al. [9] developed a deep learning-based anomaly detection approach for Industrial Internet of Things (IIoT) systems by analyzing sequential packet data. The method learns normal communication patterns from periodic data sequences and identifies deviations as anomalies without requiring additional feature engineering. The model was tested using

real-world industrial datasets and achieved accuracy of 79.6% at the application layer and 80.9% at the transport layer. The study highlighted the effectiveness of sequence-based models for detecting cyber threats in networked environments. Song, et al. [10] proposed an intrusion detection system that integrates both network-level and equipment-level information to distinguish between cyber-attacks and system faults in railway communication systems. The approach was validated using a hardware-in-the-loop simulation platform for Communication-Based Train Control (CBTC) systems. By jointly analyzing communication behavior and device conditions, the system achieved a high true positive rate of 97.64%, improving the reliability and safety of railway operations. Alabe, et al. [11] introduced a two-stage deep learning model for anomaly detection that combines autoencoder-based feature extraction with Long Short-Term Memory (LSTM) networks. The autoencoder compresses high-dimensional data into a latent representation, which is then processed by the LSTM to capture temporal dependencies. Anomaly detection is performed based on reconstruction error, allowing the model to identify deviations from normal patterns. The approach achieved high accuracy and demonstrated strong capability in handling time-series sensor data. Choi, et al. [12] explored unsupervised anomaly detection in industrial control systems using a composite autoencoder-based model. The approach was designed to identify abnormal behavior without relying on labeled datasets, making it suitable for real-world environments where labeled fault data is scarce. By learning the normal patterns of system operations, the model was able to detect deviations in both temporal and value-based characteristics. The results indicated that the proposed method can effectively support real-time monitoring and improve system reliability.

Zhao, et al. [13] proposed a hybrid deep learning framework that integrates one-dimensional Convolutional Neural Network (CNN), Bidirectional Long Short-Term Memory (BiLSTM), and Particle Swarm Optimization (PSO) for anomaly detection. The model leverages CNN for feature extraction, BiLSTM for capturing sequential dependencies, and PSO for optimizing model parameters. The approach was evaluated on industrial datasets and demonstrated superior performance in detecting complex and hidden anomalies, particularly in scenarios involving stealthy attacks. Park, et al. [14] introduced a multi-labelled hierarchical classification model for intrusion detection in railway communication systems. The model is capable of identifying both the presence and type of attacks using previously classified data. Performance evaluation showed that the approach achieved a very high F1-score and significantly reduced detection time compared to conventional classification methods, making it suitable for high-speed railway communication environments. Semenov, et al. [15] proposed a multi-level monitoring system based on clustering techniques such as Density-Based Spatial Clustering of Applications with Noise (DBSCAN) and Local Outlier Factor (LOF). The system is designed to categorize operational data into different groups and identify anomalies based on deviations from normal clusters. The results demonstrated that the approach effectively detects abnormal patterns in system parameters and supports predictive maintenance by providing early warnings of potential failures.

3. PROPOSED SYSTEM

The system architecture is designed as a hybrid framework that combines semantic text representation with interpretable machine learning models for railway communication security classification. It consists of an offline development pipeline and an online deployment pipeline. Initially, raw communication data is ingested from structured sources and processed using natural language preprocessing techniques to clean and normalize the text. The processed data is then transformed into dense SBERT based on the MPNet architecture, enabling the capture of contextual and linguistic relationships. These embeddings are used as input features for multiple classification models, including DNDT, DTCCP, and RuleFit. DNDT captures non-linear decision boundaries, Decision Tree CCP provides a pruned and efficient tree-based structure, while RuleFit combines rule-based reasoning with linear modeling for enhanced interpretability. All models are trained and evaluated using train-test split

strategies, and their performance is compared using metrics such as accuracy, precision, recall, and F1-score. Among these, RuleFit is selected as the final model due to its superior performance and transparent decision-making capability. The system incorporates a feature caching mechanism to store computed embeddings, reducing redundant computations and improving efficiency.

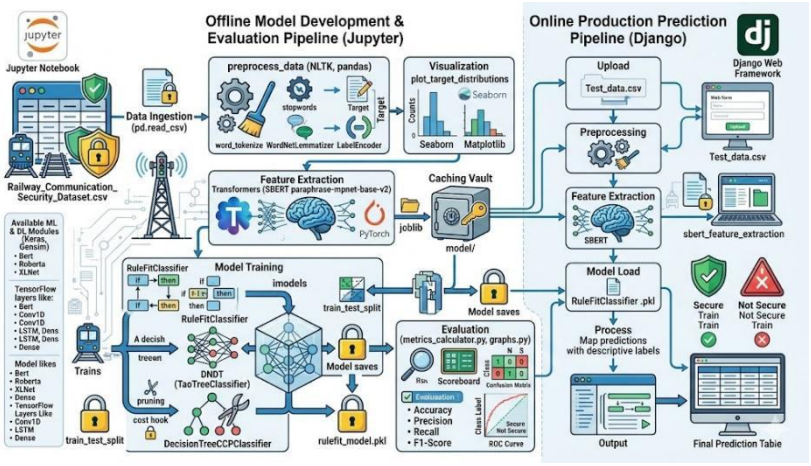


Fig. 1: Proposed system architecture

Evaluation results are visualized using graphs and confusion matrices to support comparative analysis. The finalized model is deployed in a Django-based environment for real-time prediction. The online pipeline processes incoming data through the same preprocessing and feature extraction steps before generating predictions. The output is mapped to meaningful labels such as Secure and Not Secure, ensuring clarity for end users. This architecture emphasizes accuracy, scalability, and interpretability, making it highly suitable for safety-critical railway communication systems as illustrated in Fig. 1 within the overall workflow.

3.1 SBERT

The type of BERT used in this research is SBERT**,** specifically the model all-MiniLM-L6-v2. SBERT is a lightweight, fine-tuned version of BERT optimized for generating semantically meaningful sentence embeddings rather than token-level embeddings. It modifies the original BERT architecture by adding a pooling layer on top of the transformer encoder, allowing entire sentences or documents to be represented as fixed-size vectors.

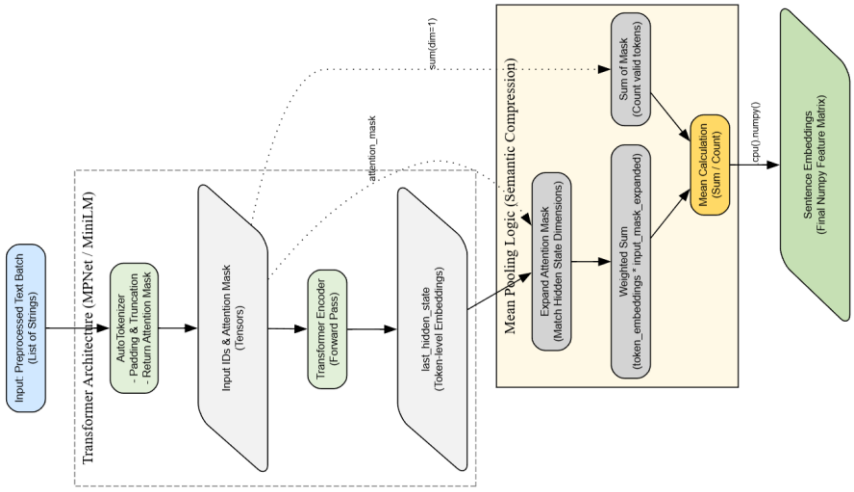


Fig. 2: Internal workflow of SBERT.

The model all-MiniLM-L6-v2 is one of the most efficient SBERT variants. It uses MiniLM, a distilled version of BERT that significantly reduces the number of parameters (only 6 layers instead of 12 or 24 in standard BERT) without compromising accuracy, as shown in fig. 2. This design makes it faster,

memory-efficient, and well-suited for applications that involve embedding large datasets. In your code, this model is loaded using the Sentence Transformer library and used to encode textual data into embedding vectors.

4. RESULTS ANALYSIS

The results section presents the key findings of the study in a clear and organized manner. It highlights the main outcomes derived from data analysis, often using tables, charts, or summaries to support the observations. This section focuses only on what was discovered, without interpreting or explaining the reasons behind the findings. It may include patterns, trends, or significant differences identified during the research. The information is usually presented logically to help readers easily understand the outcomes. It provides a factual summary of the research results.

Fig. 3 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.

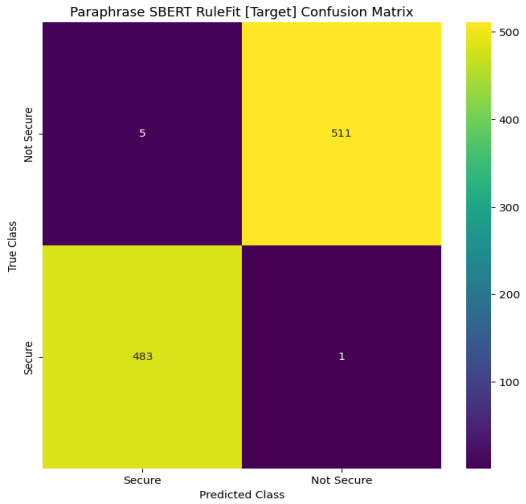


Fig. 3: Proposed Paraphrase SBERT RF confusion matrix.

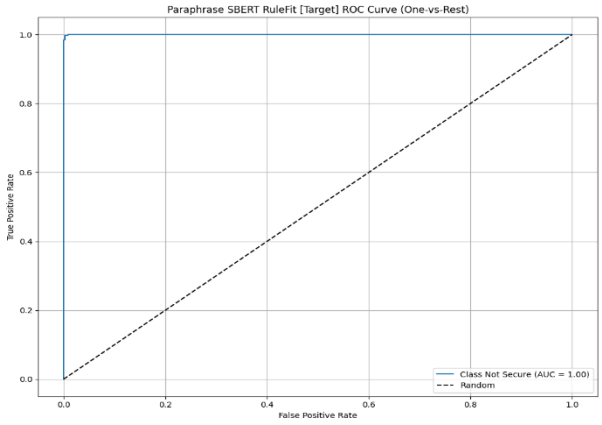


Fig. 4: Proposed Paraphrase SBERT Rule Fit ROC curve.

Fig. 4 presents ROC curves Plot 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.



Fig. 6: Batch Prediction with uploading test data.

Fig. 5 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 [Target]	48.4	24.200	50.000	32.615
DNDT [Target]	97.8	97.822	97.779	97.797
RF [Target]	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 introduces an effective solution for railway communication anomaly detection by combining semantic text embeddings with interpretable rule-based classification. By utilizing Paraphrase SBERT, the model captures deep contextual relationships in communication data that conventional approaches such as DNDT and DTCCP often fail to identify. The model achieves high performance with an accuracy of 99.4%, precision of 99.39%, recall of 99.41%, and F1-score of 99.40%, demonstrating its reliability in classifying messages into "Secure" and "Not Secure" categories. Its rule-based structure enhances interpretability, making the decision-making process transparent and suitable for safety-critical environments. The integration of SBERT embeddings enables a richer semantic understanding of textual data, improving detection capability. The model also exhibits strong robustness across varying communication patterns.

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] Hyundai Rotem; Responsible for Safety and Operational Efficiency with Smart Technology, Hyundai Rotem's Health-Based Maintenance (CBM) System. Korea. 2024.

[5] Kim, G.; Kim, H.; Koo, J. A Study on Cepstrum Analysis for Wheel Flat Detection in Railway Vehicles. J. Korean Soc. Saf. 2023, 31, 28–33.

[6] 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

[7] 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

[8] 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

[9] 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

[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] 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

[12] 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

[13] Zhao, X.; Zhang, L.; Cao, Y.; Jin, K.; Hou, Y. Anomaly Detection Approach in Industrial Control Systems Based on Measurement Data. Information 2022, 13, 450. https://doi.org/10.3390/info13100450



[14] Park, S.; Choi, J.-Y. Hierarchical Anomaly Detection Model for In-Vehicle Networks Using Machine Learning Algorithms. Sensors 2023, 20, 3934. https://doi.org/10.3390/s20143934

[15] Semenov, I.; Swiderski, A.; Borucka, A.; Guzanek, P. Concept of Early Prediction and Identification of Truck Vehicle Failures Supported by In-Vehicle Telematics Platform Based on Abnormality Detection Algorithm. Appl. Sci. 2024, 14, 7191. https://doi.org/10.3390/app14167191