Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 47 No. 02 (2026)

Explainable and Secure Cyber Attack Detection in Railway Industrial Control Systems using Temporal CNN

S Ramana Reddy [1], Chepuri Yamini [2]

[1] *Associate Professor, Vignan Institute of Technology and Science, Deshmukhi, Telangana, India*

[2] *Student of PG, Department of AI & DS, Vignan Institute of Technology and Science, Deshmukhi, Telangana, India*

Abstract:- In this paper we have proposed a layered framework for Industrial Railway Signal Control System defence against the cyber threats. Using the temporal CNN data and SCADA signal control system real time data we applied various machine learning techniques for knowledge pattern extraction. The adaptive framework also enables us to enforce various industrial standards and policies along with ML methods. Applied several metrics and features for better classification of cyber threats in this work. All the classification algorithms performance evaluation done. In this work we made to explore Cyber Security levels over industrial railway control systems towards security perspective.

Keywords*: Cyber attacks, Control systems, temporal, Heat maps, K-mean, DBSCAN, Outliers.*

1. Introduction

Railway Industrial Control Systems (ICS) includes signaling, interlocking and train control treating these units as cyber physical systems [4]. The increased demand of inventing modern techniques is to overcome vulnerabilities and cyber attacks [2]. Providing immutable ledgers Blockchain maintains verifiable records with sensor data as highly configurable and traceable [13]. Enforcing smart contracts with cryptographic credentials improves the role based access control in ICS [5]. Considering the trackside equipment, substations, stations and control centers as railway assets manages trusted communication networks over geographically dispersed assets [7]. The open networks in industrial railway network system revitalized with BlockChain providing features like decentralization, tamper-proof, secure framework that reduces failures and protecting crucial data with consistent cyber security protocol [11][6]. The temporal data analytics handles time-series data from sensors, logs and signaling devices for effective prediction and decision support system management [8]. The advanced machine learning techniques like Neural Networks and Fuzzy logic focus over continuous signal data transformation studies with improved accuracy using wavelet transformation methods [9]. For processing and analyzing railway control systems real-time data require scalable cloud services which overcomes risks with improved virtual monitor assistance by third parties [12]. The edge computing and IoT integration with track infrastructure and signal systems reduces cost results light weight communication modules for less failure collaborative network groups using wireless technology [1][3]. AI adoption turns signal system to more proactive with high energy resilience towards stable railway operations [10].

2. IRSCS Cyber Security

IRSCSS (Industrial Railway Signal Control System) cyber security is a key concern for research. Industrial railway control system works over signal management, railway track interlocking, SCADA, train control and traffic management systems. The network is highly interlaced with open networks hence vulnerable to spywares and hacker attacks.

The cyber security is essential to safe guard the digital data of industrial railway control systems. Various security measures need to be considered for effectively manage this layered cyber security architecture of IRSCS Cyber

Security. Table 1 gives an insight into various levels of measures to enhance cyber security over signal data. A recent advancement in learning systems which continuously are multi standardized to analyze several concepts of domain in several perspectives.

Table 1: Levels of IRSCS Cyber Security

Layer Name	Description
Governance of Standards	Cyber Security established in front of fire walls to prevent cyber crimes at early stages. In this layer various standards like IEC - 62443(Industrial Control Systems Security) ISO 27001 (Information Security Management) EN 50126 / 50128 / 50129 (Railway Safety Life Cycle Standard) NIS2(EU) European Region Cyber Law Enforcement Standard TSA(US) USA Region Cyber Law Enforcement Standard All these Standards are collective protocols developed to meet real-time modern cyber security challenges.
Risk Assessment	Threat Detection Modeling Rail operations risk analysis Asset classification and risk assessment Safety control measures operational RA OT Security IT Security Safety Engineering parameters Incident Registers and Response monitoring Confidentiality RA Track real time Risk Assessment (RA)
Network Architecture Segment Security	Cooperate Distributed Operational Technology Centralized DMZ Zone alarms over Safety critical systems Firewalls management over SCADA Stock privacy mangers Conduit Model Maintenance
Access Control and Identity Management	Role Based Access Management Multi Factor Authentication Privileged Access Management Vendor Access Rule managers
System Security Shield	Service Port level security Protocol enforcements Router shielding Secure line management (SCADA, PLC, HMI) Application white list generators Secure boot and firmware integrity checks
Monitoring Detection Logging	Network monitoring Anomaly detection Railway operations session trackers Centralized logging system Integrated Alerts over operational workflows
Vulnerability Management	Asset Inventory Manager Firmware Vulnerability Assessment Software Vulnerability Assessment Risk based patch system Compensate collector Vulnerable Activity Scanners

Layer Name	Description
Incident Response and Resilience	IR Plans Operational Signal IR register Fail safe signaling Resilient Operations Manager Secure backup manager Testing strategies Rapid restore schedulers
Supply Chain Management	Contract Privacy Manager Supply Chain Life Cycle security SBOM Controlled update and validation Deployment Service Security updater

3. Proposed System

The Industrial Railway Control System architecture is shown in figure 1. The layered model has three layers, each layer interlaced with various modules associated with set of services. This model provides a suitable communication framework for real-time wireless networks like Industrial Railway Signal Networks.

Application Layer

An enterprise level corporate collaborated service module with ERP software application framework intensive focus over security concerns. The communication through web improved with cyber security policies enforcement over e-mail communication. The HR modules totally focus over railway signal network resource optimization and tuning with precise security. The resource management also governed with corporation strategies. The planning module models the communication architecture under the margins influenced with domains like Cyber Security, AI and Machine Learning.

Intrusion Detection Layer

Major collection of network security measures and protocol oriented services are managed in this layer. Providing total control over firewalls and IDS improves the stability of network traffic. Support historical trend analysis tools to perform knowledge learning over time series data. Manages signal operations smoothly over jump servers. The patch management always upgrades security systems with latest technologies.

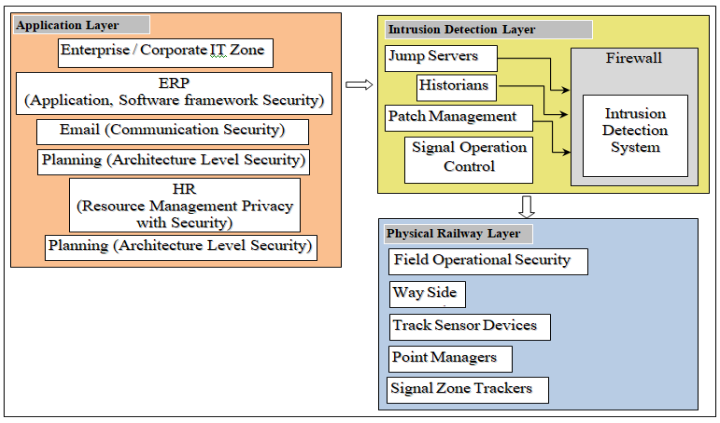

Figure 1. Industrial Railway Control System Architecture

Physical Layer

The low level layer manages control and communication among physical entities of IRCS. 'Field Operational Security' manages the security essentials over railway field structures. Enable to track wireless interceptions, signaling vulnerabilities and interlocking attacks. Majority attacks registered over track status real-time data.

Various encryption schemes applied in this module to safeguard VCU (Vehicle Control Units), OT (Operational Tracks) and Way Side Objects (WSO). The track sensor IoT equipment is supported with security protocols of edge computing and cloud computing. Enforcing IEC-62443 standard using software modules to enhance the signal zone trackers security. Arranging Tamper alarms, cable security and data integrity monitors. The fiber cable encryption standards are enforced in this layer.

4. Result Analysis

ROC for Classification models

In this work we adopted multiple classification algorithms to classify the cyber attacks over IRCS data sets. The ROC curve shows that Random Forests are extensive to handle large real-time temporal data sets generated from CNN analysis. But we observed latency in execution a bit hard for interpretation. The accuracy given is 56.5% for random forests in cyber threat classification. When there are attacks on a specific data sets showing exponential increase logistic regression based classification gives us better groupings supporting 90.7% of accuracy in classification. Due to high dimensionality and Sparsity in time series data generated from IRCS modules SVM is well suited for classification of cyber attacks. They are faster and capable to handle wide dimensionalities with an accuracy of 95.6% highly suitable for IoT enabled signal systems, way side devices and train operation device data cyber threat classifications.

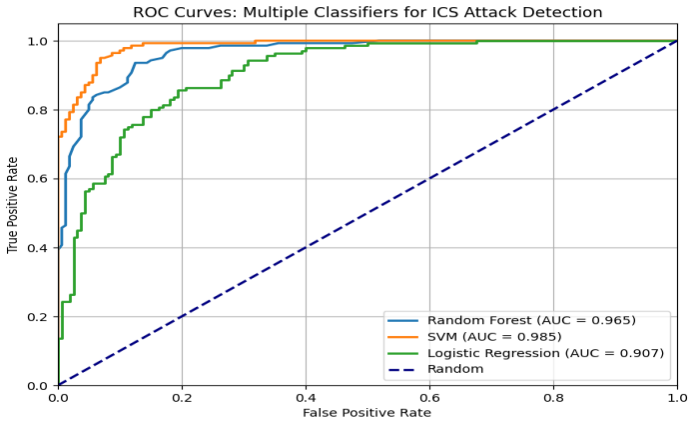

Figure 2. Accuracy rate among SCM systems

Cyber Attack detection analytics

The IRCS network anomalies are classified into Signal spoofing, Timing faults, Occupancy errors and Point malfunctions. The figure 3 shows score analysis of cyber attacks reveal that majority of attackers target signal timing control units for altering unauthorized.

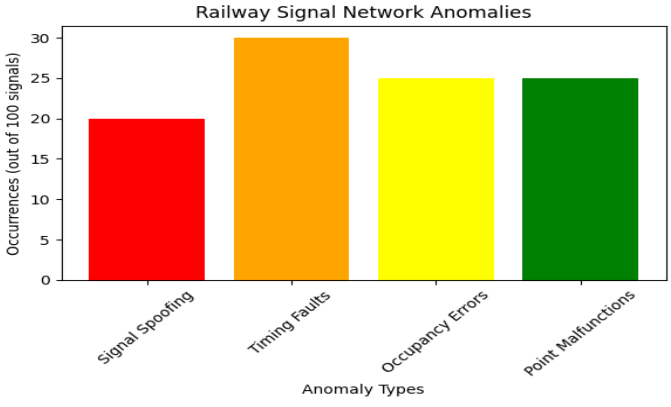

Figure 3. Signal Network Anomalies

Heat Map Study of Threats

The heat map analysis cyber threats shown in figure 4 clearly depict the real time vulnerabilities over physical layer of IRCS. The attacks majorly upload malicious codes and credential stealing over way side trackers. In SCADA networks it is noticed high risk of interceptions and injection attacks. Also GSM-r and SIM data network attacks are causing exploiting risks up to 36% to sensitive data.

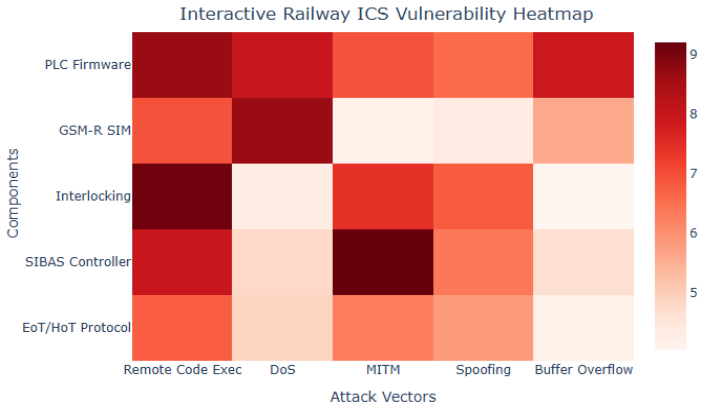

Figure 4. IRCS Vulnerability Heat Map

The attacks majorly upload malicious codes and credential stealing over way side trackers. In SCADA networks it is noticed high risk of interceptions and injection attacks. Also GSM-r and SIM data network attacks are causing exploiting risks up to 36% to sensitive data.

Table 2: IRCS Attack rates summary

IRCS unit	RC Error	DoS	MIM	Buffer Overflow	Spam	Spoofing
PLC Firmware	1918	87	46	780	56	24
GSM	855	66	43	210	27	19
SM	1178	53	25	27	11	8
Interlocking	798	37	56	16	21	11
SIBAS	652	12	9	10	5	3
EoT	1723	47	18	22	12	15
WST	1160	26	12	21	6	2

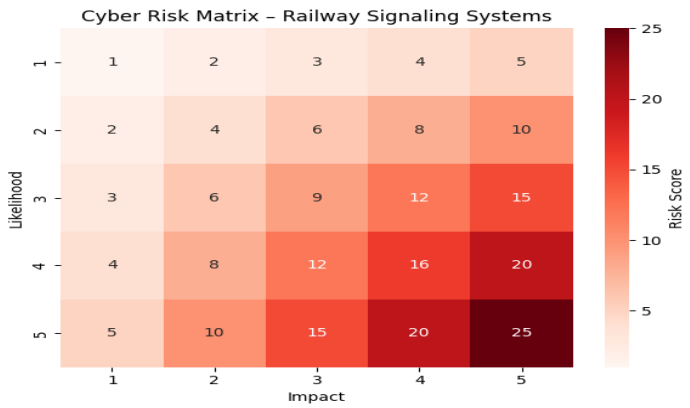

Figure 5. Cyber Risk Analysis

The figure 7 shows the cyber attack risk analysis over IRCS and their impact over control system activities based on score factor analysis. It is noticed that factor of data vulnerability increases the rate of attack impact on sensitive data. The IoT devices are more vulnerable to open network attacks showing high impact of cyber attacks. More care should be taken over WST devices. Regular firewall updates and new patches to security software modules. Applying latest network security standards improve the quality of service in IRCS.

Cluster Analysis

The cluster analysis conducted using K-mean, CLARAN, DBSCAN and HCA over training data related to SCADA signal network.

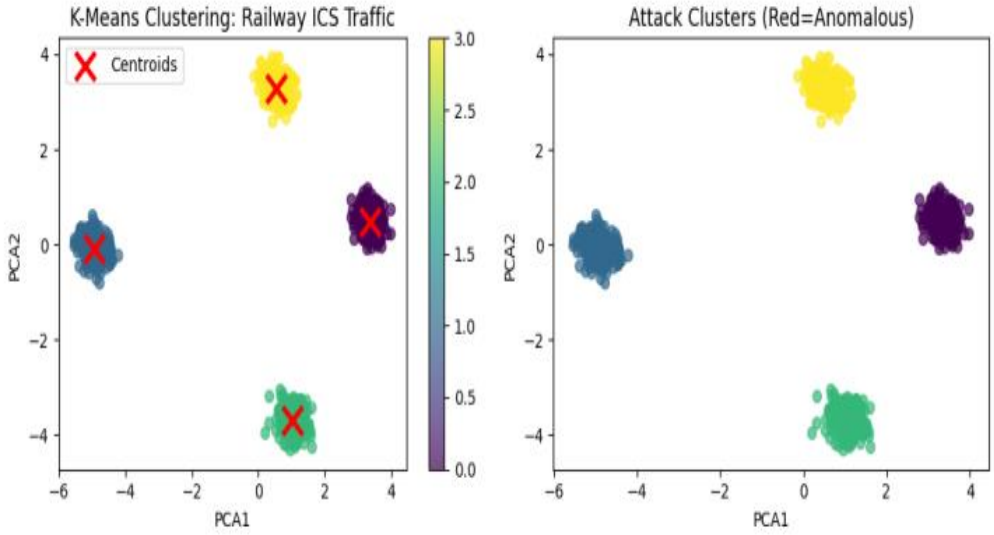

Figure 6. Clustering based Rail alerts

This analysis helps to group cyber attacks based on similarity metrics. The algorithms examined traffic patterns, signal controls, payloads, time framings and impact vectors. The table below gives the various algorithms approach to predict clusters of information over IRCS.

Table 3: IRCS Attack rates summary

Clustering Scheme	Measures	Attacks clustered
K-mean	Log data, network packet metrics	Multi stage cyber attacks, risk factors
DBSCAN	Network loads, traffic states	DDoS, MIM, Spoofing
Hierarchical Clustering	Data frames, frequencies	Trojans, Spywares, Injections
PAM, CLARAN	Network hyper dimensional data	cyber threats, hijacking, collisions, malicious attacks, spams

ROC Analysis

The ROC evaluated binary classifiers for cyber attack detection over IRCS. The plotted curve shows true positive rate over false positive rate values using given thresholds. From normal operations to train track control automation several cyber threat occurrences increased the TP values of curve. The random classifiers showing uniform sensitivity to cyber threats during operational maintenance. Curve closer to top corner indicates better performance. The AUC must maintain around 1.0 for reliable railway ICS security.

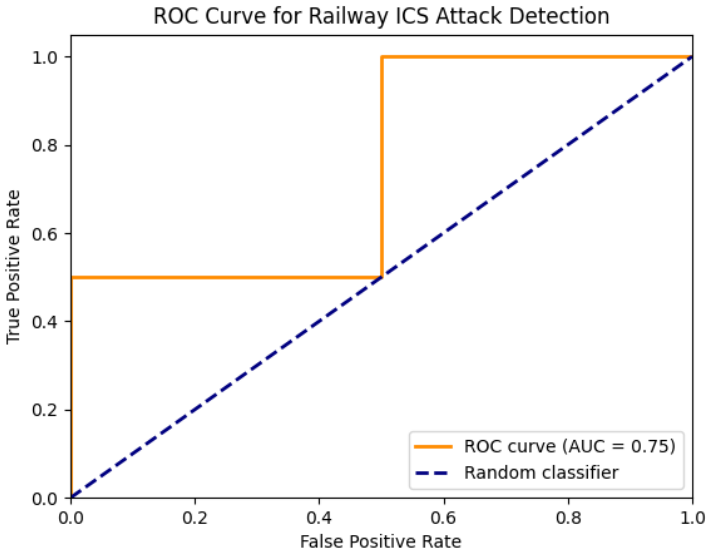

Figure 7. Cyber Attack Analytics

The TPR is the rate of correctly detected attacks. FPR indicates misclassified attacks triggered. The ratio indicates the ROC performance. The XG-Boost algorithm is highly adoptable for ROC analysis using auto encoders. Threshold selection is an important criteria for model performance.

5. Conclusion

In this work cyber attacks detection over Railway Industrial Control Systems using Temporal CNN data sets done. The SCADA networks provided industrial standard metrics for signal control machines generated data. The layered model gives us transparency of basic building units of IRCS system. From the application layer each layer is maintaining data dependency over lower layers. The random forests are very effective in handling large data sets classification based on varied cyber threat classifiers. SVM gives 95.6% performance in classification of linear behavioral threats. We have noticed more amount of signal network faults raised due to 'timing failures'. The heat maps provided an insight into IRCS vulnerabilities. Also the risk analysis conducted in this work revealed risk and impact ratios. The clustering of various cyber attacks using wide variety of algorithms projected different knowledge patterns.

The ROC analysis significantly proved the role of threshold values in identifying correct class members in a group. Hence the application of machine learning algorithms over IRCS helps in better decision making to improve cyber security over the railway networks.

References

[1] Pavlo Holoborodko, Darius Bazaras, " Future Rail Signaling: Cyber and Energy Resilience through AI Interoperability", Journal of Sustainability, MDPI, ISSN: 2071-1050, Vol.17, Issue-10, 2025.

[2] M Tarun, M Lakshmanrao, M Vivekvardhan, "Enhancing Railway Operations through Blockchain: A Secure and Transparent Future", IJCSE, ISSN: 2583-9055, Vol.3, Issue-2, pp: 189-196, 2025.

[3] Zoran Pavlovic, Ana Savic,"Application of Blockchain in the Railway Company", 24-ISIJ Symposium, ISBN: 975-672-67-9, pp:128-131, 2025.

[4] Md. Nurul Absar, Md. Eusuf Jamil, “Implementation of Blockchain Technology in Railway Industry of Bangladesh", ICIEOM Conference, IEOM Publisher, DOI: 10.46254/AN15.20250365, pp: 1642-1653, 2025.

[5] Rahma A Alizahrani, John M Easton," A Secure and Scalable Blockchain Framework for Data Sharing and Cost Distribution in Railway Condition Monitoring", IEEE-Access, Vol.13, pp: 151491-151511, 2025.

[6] A Bruzzone, A Giovannnetti, S Rajendra Gangar, "Blockchain for Secure Railway Signal Communication & Protection of Critical Infrastructures", IMMSM Conference, ISSN: 2724-0363, DHSS, 2024.

[7] Palvoc Zoran, “Improving cyber security in railway traffic and transport using Blockchain technology", ICSERR-24, ISBN: 978-86-6055-188-9, 2024.
[8] Xiong Liang, Yang Lu, Yingka Liu, "Enhancing Security in Recommendation Systems with Blockchain Technology", ACM-TURC Conference, ISBN: 979-8-4007-1011-7, pp: 132-137, 2024.
[9] Satya N Gupta, "Blockchain and Future Communication based Decentralized Train Control System", AKEC International Journal of Technology, Vol.13, Issue-2, pp; 1-10, 2023.
[10] Alessia Tardivo, C Sanchez Martin, "A study of Blockchain adoption in the rail sector", Transportation Research Procedia Journal, Elsevier, ISSN: 2352-1457, Vol.72, pp: 1396-1403, 2023.
[11] Hengjijang Liu, Yunshui Zheng," Application of Blockchain technology in railway information sharing research", 5th ICCISAT conference, DOI: 10.1117/12.2656908, 2022.
[12] Micheal Kuperberg, "Scaling Blockchain based Railway Control System Prototype for Mainline Railways: a Progress Report", Sicence Open Journal, Arxiv Publishers, 2021.
[13] Gansen Muniandi, "Blockchain enabled secure crowd sensing for track side infrastructure information collection and validation in railway signalling data preparation", IET Blockchain Journal, WILEY Publishers, ISSN: 2634-1573, DOI: 10.1049/blc2.12002, pp: 16-32, 2021.