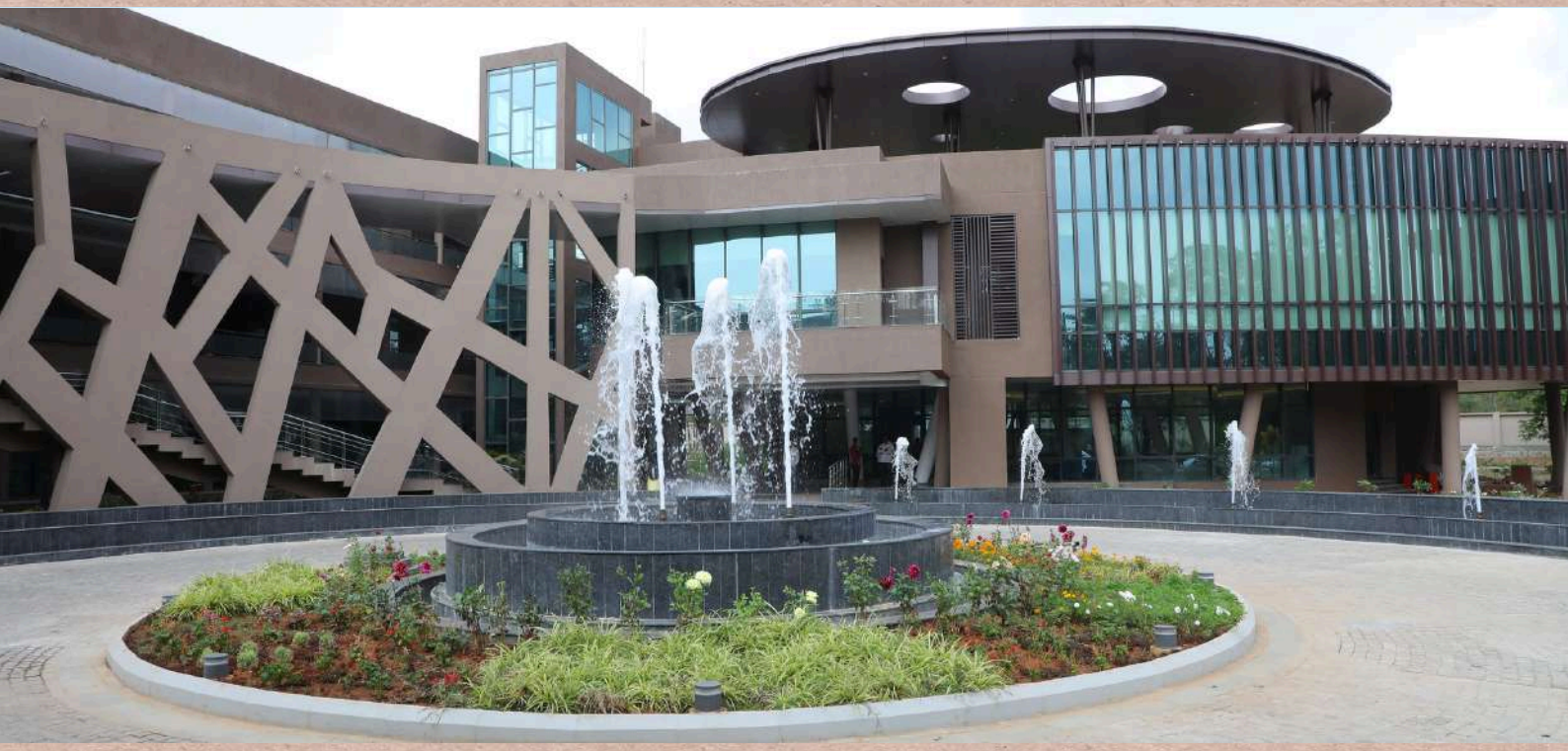
Edition #10

October 2025

INDIAN RAILWAYS INSTITUTE OF FINANCIAL MANAGEMENT(IRIFM)

THE FISCAL TRACK

www.irifm.indianrailways.gov.in



INSIDE THE ISSUE

ARTICLE 1

Navigating the next disruption:
Quantum computing
by K. Sitharamaraju, Dean cum Sr. Prof/IRIFM

EVENTS AT IRIFM

- Appreciation course for RPF Probationers
- 5th Forensic Accounting course
- Sr. Professional course for PCMDs
- Refresher course for supervisory staff and training on HRMS Module.
- Conducted four webinars.

ARTICLE 2

Cyber Security:
Staying vigilant in the Digital era
by Nikhil, IRMS/A Probationer, IRIFM

Best practices in Cyber Security

SPECIAL FOCUS

In commemoration of Cyber Security Awareness Month, this edition highlights the transformative role of Artificial Intelligence (AI) in IR through three special focus articles:

1) AI in Public Procurement:
Empowering Officers, Enhancing Transparency
By Nav Goel, GM/Finance/IRFC.

2) AI-enabled detection tools for financial frauds in the Railway ecosystem by S Santhi Raju/ADG/IRIFM.

3) Potential areas of use of Artificial Intelligence in Indian Railway Health Services
by Dr Arunangshu Sarkar/SPHM/IRFM.

BUDGET AT A GLANCE

Freight Revenue analysis over the last ten years.

"Digitization is the first step; digital transformation is the journey."

– World Bank Digital Development Report

FROM DG'S DESK

Dear esteemed readers,



The month of October is observed globally as the "cyber security awareness month". The focus of this edition is to be a part of #CyberJagrit Bharat by creating awareness amongst our readers on the digital strides and the importance of cyber hygiene. Best practices on cyber security are shared. There are write ups which dwell on the scope of the three top emerging technologies in 2025 i.e., AI, Quantum Computing, and Cloud & Edge computing.

"Power to Empower" the tagline was given by the Government of India in the year 2015 to transform India into a digitally empowered society by providing services electronically and improve online infrastructure. A key component has been to promote digital literacy and adopt digital platform.

India's digital economy has emerged as a significant contributor to its economic growth. The Indian economy has been digitalising at a remarkable pace over the last decade. It's share in GDP has increased from 4.5% in 2014 to 12 % in 2024.In 2025 it is expected to grow to 13.42%. According to the State of India's Digital Economy Report 2024, India is the third largest digitalised country in the world in terms of economy-wide digitalization. India's digital economy is expected to grow almost twice as fast as the overall economy, contributing to nearly one-fifth of national income by 2029-30. This means that, the share of digital economy will become larger than that of agriculture or manufacturing in the country.

Key growth drivers include the rapid adoption of AI, cloud services, and the rise of global capability centers (GCCs). In the short run, the highest growth is likely to come from the growth of digital intermediaries and platforms, followed by higher digital diffusion and digitalisation of the rest of the economy.

In the railway sector, the internet of things, cloud computing, extensive data analytics, and mechanisation and robotics have accelerated the digital transformation.IR has adopted digitalization in all aspects of its functions: passenger data systems, accounting applications, management of data of its human resources, predictive maintenance, train signals, ground control systems, procurement, unreserved ticketing methods to name some. We are implementing Industry 4.0 in our manufacturing facilities, deploying drone-mounted cameras and 3D scanning of river beds to examine bridges and contemplating use of drones for rail maintenance in the future.

As the digital footprints become all encompassing, the vulnerability of data and digital assets to cyber threats also increases.Indian Railways is a part of the National Critical Information Infrastructure, making robust cyber security essential for national security and resilience. A cyber attack could disrupt signalling, control systems, and operations, leading to delays, cancellations, or even accidents, which is a major safety concern. Sensitive data, including passenger information, financial records, and proprietary operational data, must be protected from breaches and theft.

With increasing digitalization, employees must be aware of the risks associated with it. Strict protocols must be followed and technology should be used securely. Digital backbone has to be protected with advanced and multi layered technology.

Budget under Plan Head 17 will have to undergo massive transformation as we start factoring the latest digital innovations. This edition attempts to focus on some dimensions of digital scope. I would encourage young readers to contemplate and write for our future editions.

In this fast-evolving tech inspired work spaces 'Digital sovereignty is as important as territorial integrity'.

As we surf the digital wave into the future, let's ride with both innovation and intention. In a world where data is gold and clicks are currency, cyber security isn't just a precaution - it's a superpower. Until next issue, may your password be strong and your firewall stronger; stay sharp, stay encrypted and don't' feed on phishing trolls.

Warm regards,

Aparna Garg, IRAS
Director General,
Indian Railways Institute of Financial Management.

RAILWAY BUDGET AT A GLANCE

INDIAN RAILWAYS FREIGHT MANAGEMENT: TRAJECTORY, VISION, AND CHALLENGES

- BY U.L.N RAO, RETD. DY.FA&CAO AND CONSULTING PROFESSOR

Introduction

Indian Railways (IR) plays a vital role in shaping India's transportation network and its economic foundation through its logistics and supply chain network, especially for bulk commodities. As India steers towards becoming a $5 trillion economy, IR's strategies for freight management, modernization, and capacity building are more crucial than ever.

This article presents a narrative account of IR's trajectory, vision, capacity-building efforts, challenges, and the impact of its freight activities.

Growth Trajectory and Performance Analysis

Indian Railways' freight performance has witnessed substantial growth over the last decade, punctuated by fluctuations due to macroeconomic factors and disruptive events like the COVID-19 pandemic. The data below summarizes freight loading and revenue across recent years.

Freight Revenue Analysis 2014-2025 to 2024-25

Year	Freight Loading (Mln Tonnes)	Revenue from Freight (₹ Mln)	NTKM (Mln)	Yield (Revenue (Rs) / Ton)	Yield (Revenue (Rs) / NTKM)
2014-15	1095.26	1031002	68170	941.33	15.12
2015-16	1101.51	1069406	65448	970.85	16.34
2016-17	1106.15	1020278	62018	922.37	16.45
2017-18	1159.55	1135235	69292	979.03	16.38
2018-19	1221.48	1225803	73852	1003.54	16.60
2019-20	1208.41	1114723	70767	922.47	15.75
2020-21	1230.94	1157384	71976	940.24	16.08
2021-22	1415.87	1392873	87182	983.76	15.98
2022-23	1509.1	1601585	95957	1061.28	16.69
2023-24	1588.06	1658806	97397	1044.55	17.03
2024-25 *	1617.38	1753024	98858	1083.87	17.73

** Data is provisional .Freight loading and revenue is taken from media and NTKM is estimated based on previous year growth.*

Performance 2014-2025				Yield (per ton)	Yield (per NTKM)
	Absolute Growth	%	Max	1083.87	17.73
Loading (MT):	522.12	47.67	Min	922.37	15.12
Revenue : Rs. Mln)	72202	70.03	Avg	976.94	16.24
Yield (Rev/ton)	142.54	15.14	Standard diviat	53.46	0.65
Inference : Movement of High rated commodities			**Inference : Consistent performance**		

RAILWAY BUDGET AT A GLANCE

Key Performance Trends

- **Freight Loading:** Increased steadily from 1095.26 million tonnes in 2014-15 to 1617.38 million tonnes in 2024-25, an absolute growth of 522.12 million tonnes or 47.67%, reflecting sustained volume growth.
- **Freight Revenue:** Rose from ₹1,031,001.5 million to ₹1,753,023.7 million over the period, a significant growth of 70.03%, outpacing volume growth indicating enhanced revenue management.
- **Yield (Revenue per NTKM):** Yield for 2024-25 is 17.73 ₹ per NTKM, reflecting an unswerving increase year on year and also there is overall growth of 17.25% over 2014-15. This suggests an exceptional increase in revenue efficiency, pricing and effective commodity mix or strategic uplift.





Inference and Comments

- The **steady rise in freight loading** confirms expanding utilization of railway freight capacity and consistent market demand.
- **Revenue growth outpacing freight volume growth** is positive, indicating successful pricing strategies or shifts toward freight with higher yield.
- The **sharp jump in 2024-25 yield** relative to historical range is unusually high and may need detailed examination for underlying growth drivers such as tariff increases, commodity mix change, or data reporting revisions.
- Minor revenue/yield fluctuations in some years are likely linked to economic conditions or operational constraints.

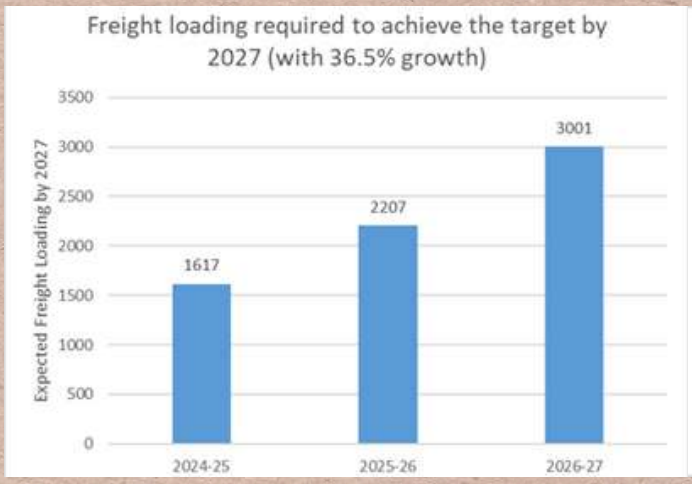
Current Status and Growth Gap

Indian Railways aims to achieve a freight loading target of 3,000 million tonnes (MT) by 2027, but as of September 2025, actuals are only 801 MT for FY 2025-26, up just 3.2% year-on-year, and 1,617 MT in FY 2024-25, which is 53.9% of the vision 3,000 MT. Given the present trajectory, this target appears extremely ambitious and would require a compound annual growth rate (CAGR) of roughly 36% for each of the next two years, as against the current average of around 4%.

RAILWAY BUDGET AT A GLANCE

Feasibility of Target

Meeting the 3,000 MT target by 2027 is extremely unlikely under current trends, barring a drastic shift in both supply and demand-side factors. Historically, doubling freight volumes within such a short period has not been achieved in Indian Railways in recent decades. The most recent action plans suggest the target date might need to be pushed to 2030-31 for even a 9.25% annualized growth.





Indian Railways can quickly boost freight by strategically expanding high-growth commodities and key freight corridors.

.....

SPECIAL FOCUS

AI IN PUBLIC PROCUREMENT: EMPOWERING OFFICERS, ENHANCING TRANSPARENCY

- BY NAV GOEL, IRAS, GENERAL MANAGER/FINANCE,
INDIAN RAILWAY FINANCE CORPORATION.



India's vast public procurement system–accounting for nearly a fifth of GDP–still relies heavily on manual tender evaluation despite digital platforms like GeM. Officers must sift through thousands of pages to verify eligibility and compliance, leading to delays and errors. The article argues that Artificial Intelligence, especially Generative AI combined with OCR and semantic analysis, can revolutionize this process by automating document reading, verification, and comparison while enhancing transparency.

In India's trillion-rupee procurement ecosystem–where transparency, value-for-money, and speed are paramount–tenders are the heartbeat. The scale is staggering: government procurement across Union, State, and PSU purchases accounts for nearly 20–22% of GDP. From defence to healthcare, rural electrification to high-speed rail, procurement shapes the country's development story.

Yet behind this machinery lies an often-overlooked aspect: the demanding nature of evaluation. Officers tasked with scrutinising tenders wade through thousands of pages–checking eligibility, verifying certificates, and comparing bids–under pressing deadlines. While platforms like GeM have digitised the front-end, the back-end is still dependent on extensive documentation.

The Evaluation Challenge

Consider this: in FY 2023–24 alone, GeM processed over ₹3 lakh crore worth of goods and services, with more than one crore product listings and 65,000 registered government buyers. Each tender receives anywhere between 5 to 25 bids, depending on its scope, with vendors uploading statutory, technical, and financial documents, often running into 2,000 pages or more.

While digital platforms have transformed access, the next step is enabling intelligent interpretation of data. Bidders upload; officers download. But evaluation is still dependent on extensive documentation often resulting in cognitive overload sometimes leading to longer timelines and inadvertent errors.

AI in Tender Evaluation

This is where GenAI–offers a breakthrough. In the present-day system, by combining Optical Character Recognition (OCR) with semantic parsing, AI engines can read, extract, and compare information at scale. What takes days for humans can be reduced to hours, with fewer mistakes and more transparency.

Imagine an AI agent that ingests bids directly from GeM or CPP or IREPS, identifies whether eligibility criteria like turnover or certifications are met, and produces a compliance matrix–flagging anomalies for human review. A dashboard highlights each vendor's status in red or green, leaving officers free to focus on exceptions rather than routine checks.

Implementable Steps for Smarter Tender Evaluation

1.Machine-Readable Bid Annexures (MRBA) - Alongside the regular PDF, bidders submit a signed JSON/XML sheet with key eligibility data–turnover, net worth, OEM certificates, BIS/ISO numbers, PAN/GST, labour registrations. This reduces parsing errors and allows deterministic, rule-based checks.

2.Trusted Data Cross-Checks - AI can link directly (read-only) to government systems like MCA-21 (company basics), GSTN (registration validity), EPFO/ESIC (statutory codes), BIS (licences), UDYAM (MSME status), and UDIN (turnover certificates). MRBA fields can be instantly verified, producing a log of matches, mismatches, or exceptions–while the committee retains the final say.

3.Clause-to-Evidence Mapping (CEM) - Tender clauses are uploaded in a structured format (e.g., "minimum average annual turnover ₹X; required document: audited financials Y/N"). AI highlights the exact page or snippet in each bid that meets–or fails–the requirement, and generates a comparative statement with links to source documents. This creates a transparent, audit-ready trail.

4.Risk & Exceptions Register (RER) - Instead of opaque AI scoring, the system maintains a visible register of issues–missing pages, expired certificates, arithmetic errors, or unusually low bids. Each flagged item requires a human decision (accept, seek clarification, or reject), embedding accountability while cutting routine workload.

5. AI-Led Rate Reasonability - Determining fair price is often the most complex task. AI can scan procurement archives across GeM, CPP, IREPS, and state systems to surface the Last Accepted Rate (LAR) for comparable works. Factoring in geography, inflation, scope, and scale, it provides committees with a benchmark range. For instance, a bridge tender in Bareilly can be compared against similar works across Indian Railways, CPWD, and PWDs in the past three years–adjusted for region and escalation.

6.National Procurement Database - On the lines of PM Gati Shakti, which integrates 1,614 data layers across 44 ministries and 36 States/UTs, a centralized procurement database of LARs can be developed. This broadens AI's learning base and ensures benchmarking is both accurate and nationally representative.

Human Oversight, AI Assistance

Concerns about AI replacing human judgment are misplaced. AI will not decide who wins a contract–it will simply remove the drudgery. Accountability will always rest with evaluation committees. AI outputs should be treated like preliminary screening reports: useful for flagging non-compliance but always subject to human verification. The government, too, can issue clear guidelines to define responsibilities and ensure audit trails.

Beyond Evaluation: Smarter Pre-Tendering

AI can also support pre-tender stages–drafting RFPs, removing contradictory clauses, and standardising evaluation formats. This is particularly valuable in departments with high officer turnover and weak institutional memory.

The Road Ahead

India's capex budget for FY25 stands at ₹11.11 lakh crore. As we aspire for Viksit Bharat by 2047, intelligent systems will be indispensable. A phased approach to AI-assisted evaluation, beginning with pilot projects and training, integrating platforms like GeM, CPP, IREPS with AI modules could complement existing policy efforts. India's public procurement is now well-placed to progress from digital file uploads to digitally intelligent systems. It must evolve from piles of paper to pillars of intelligence. AI won't replace evaluators. Instead, it will reduce routine workload, minimize inadvertent delays, and support officers in faster decision-making. As the government pushes for faster infrastructure delivery, timely fund utilization, and clean governance, AI can be a trusted aide behind every fair and efficient award.

.....

Disclaimer: Views expressed are personal and do not reflect the official policy/ position of the Institute.

SPECIAL FOCUS

AI-ENABLED DETECTION TOOLS FOR FINANCIAL FRAUDS IN THE RAILWAY ECOSYSTEM

- BY S SANTHI RAJU, IRAS,
ADDITIONAL DIRECTOR GENERAL/IRIFM.



This article highlights how Indian Railways can leverage Artificial Intelligence to transform financial vigilance from a manual, reactive process into a proactive, data-driven system. By integrating AI tools with core applications like IPAS, IREPS, and e-MB, Railways can detect anomalies, prevent fraud, and strengthen transparency and governance across its vast financial operations.

Introduction

The Indian Railways, one of the largest public sector organizations in the world, handles an enormous volume of financial transactions every day – from procurement and works contracts to payroll, passenger, and freight earnings. With expanding digital platforms and interlinked financial applications, safeguarding financial propriety has become a critical institutional priority. Drawing on the insights and case studies contributed by participants of the Forensic Accounting and Financial Investigations Training Programme at the Indian Railways Institute of Financial Management (IRIFM), this article explores the emerging potential of Artificial Intelligence (AI) in detecting financial frauds, anomalies, and irregularities across the Railway ecosystem.

1. Present scenario in Indian Railways

Currently, Indian Railways relies primarily on manual and Excel-based analysis for detecting anomalies and irregularities. Data is usually extracted periodically from core applications such as IPAS, IREPS, HRMS, TAMS and e-MB through reports or CSV (Excel, PDF and Text) exports.

Officers and staff perform cross-checks by:

- Using pivot tables and formulas in Excel to identify mismatches in work bills, vendor payments, or revenue data.
- Conducting sample-based audits to verify suspected irregularities.
- Preparing ad hoc reports to identify duplicate transactions or overpayments.
- Comparing procurement and payment data manually across divisions or cost centers.

While this approach provides basic oversight, it is time-consuming, reactive, and prone to data omissions. The absence of automated inter-system integration and real-time alerts means that irregularities are often detected, long after the transaction has occurred.

The transition to AI-based systems can shift the focus from post-facto audit to proactive surveillance, enabling faster response and preventive action.

2. The emerging role of AI in Financial Vigilance

AI and Machine Learning (ML) techniques enable early detection of irregularities by identifying hidden patterns, deviations, and correlations that may go unnoticed through manual audit processes. Unlike static rule-based systems, AI models evolve continuously by learning from historical data and real-time inputs.

In the Railway financial domain, AI can be instrumental in identifying:

- Over-invoicing or duplicate billing by contractors.
- Abnormal tender rates or irregular variation orders.
- Irregular refund patterns in passenger and freight transactions.
- Unauthorized access or manipulation in accounting systems.
- Collusive behaviour among vendors and internal stakeholders

3. AI-driven Fraud Detection Tools and their Railway applications

a) Anomaly Detection Models
AI models analyze historical patterns in expenditure, billing, and contract performance to flag outliers.
Example: Integration with IPAS (Integrated Payroll and Accounting System) can identify duplicate or excessive payments, unusual advance adjustments, or inflated debits in specific cost centers.

b) Predictive Risk Scoring
Machine learning can assign risk scores to vendors and contracts based on prior irregularities, financial performance, and litigation history.
Example: Linking this with IREPS (Indian Railways E-Procurement System) helps flag potentially high-risk tenders during evaluation itself.

c) Graph-based Analytics
AI can map relationships between officers, contractors, and projects using graph algorithms to detect collusion networks.
Example: By linking vigilance and contract databases, repeated associations between specific evaluators and vendors can be auto-flagged.

d) Natural Language Processing (NLP)
NLP tools scan text data – such as tender clauses, correspondence, or noting files – to detect deviations from standard templates or the inclusion of risky terms.
Example: Integration with e-Office / File Tracking Systems (FTS) can identify unauthorized modifications in tender documents.

e) AI-based Document Verification
Combining Optical Character Recognition (OCR) and AI-based image comparison helps detect tampering in scanned vouchers, bills, or work measurements.
Example: Integration with e-Measurement Book (e-MB) ensures that only system-authenticated entries are processed for payment.

f) Behavioral Analytics
AI models analyze user activity patterns to detect unusual login times, repeated data overrides, or unauthorized workflow bypasses.
Example: Integration with IPAS or HRMS can reveal digital signatures used beyond normal hours or outside authorized locations.

4. Integration framework within the Railway ecosystem

AI Function	Target Railway Systems	Expected Outcome
Anomaly Detection	IPAS, TAMS	Detect irregular transactions and misclassifications
Predictive Risk Scoring	IREPS, CMS	Flag high risk vendors and projects
Graph Analytics	Vigilance DB	Identify collusive networks
NLP Document Review	e-Office, FTS	Flag altered tender clauses
OCR & AI Verification	e-MB, CMS	Detect tampered or duplicate documents
Behavioural Analytics	IPAS, HRMS	Identify suspicious user behaviour

5. Forensic and Analytical Tools in use

Global and public-sector audit organizations already employ powerful forensic tools that can be adapted for the Railway environment:

- IDEA (Interactive Data Extraction and Analysis): Used for large-scale audit data analysis and sampling.
- ACL / Galvanize: For automated transaction testing and control monitoring.
- Power BI / Tableau with AI visuals: For real-time fraud analytics dashboards.
- SAS Fraud Framework: Provides continuous monitoring and fraud scoring models.
- IBM Watson Analytics: Detects complex anomalies using cognitive AI.
- Python-based Open Source Libraries (Scikit-learn, TensorFlow, PyCaret): Offer flexible, in-house AI development for Railway-specific workflows.

Integration of these with Indian Railways systems (IPAS, IREPS, HRMS, CMS) through secure APIs can create a unified fraud detection and analytics ecosystem.

6. Case Study: AI-based detection of financial irregularities in Contractor payments

Background

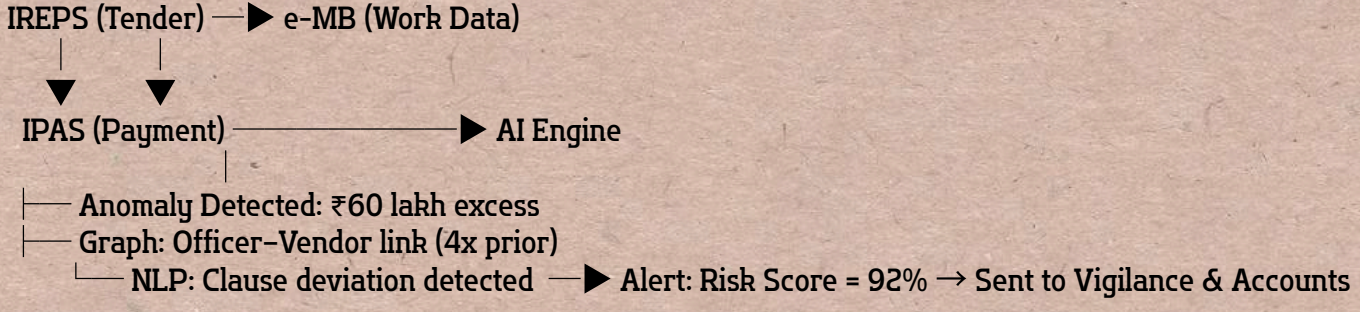
A construction division sanctioned a ₹4.5 crore track renewal contract. Payments were processed through IPAS, based on data from IREPS (tender) and e-MB (work progress).

The AI-based dashboard flagged one contractor's bill with a "High Anomaly Risk" – confidence level 92%.

Data Overview

System	Key Data Points.	Observations
IREPS.	Contract Value: ₹4.5 Cr.	Base agreement
e-MB.	Work Executed: ₹4.5 Cr.	Matches schedule
IPAS.	Payment: ₹5.1 Cr	Excess ₹0.6 Cr
CMS	Variation Register: None	No approved variation
HRMS	Officer Handling: Same across 4 prior contracts	Pattern detected

Detection Workflow



AI Dashboard Snapshot (Sample Output)

parameter	Expected	Actual	Anomaly %	Risk
Contract Value	Rs 4.50 Cr	Rs 4.50 Cr	0 %	Normal
Payment	Rs 4.50 Cr	Rs 5.10 Cr	+13.3%	Crictical
Variation Order	Yes	No	--	Critical
Officer - Vendor Link	0-1	4	--	High
Text Clause Deviation	None	Found	--	Moderate

Outcome

- ₹60 lakh excess payment detected automatically within 24 hours.
- AI revealed a repetitive officer–vendor pattern across multiple tenders.
- Disciplinary and recovery actions were initiated.

Key learnings

- AI connected three databases (IREPS, IPAS, e-MB) to detect the anomaly.
- Detection time reduced from months to hours.
- Scalable model – applicable to fuel purchases, AMC contracts, and refund monitoring.

7. Governance and ethical oversight

Implementing AI for financial vigilance must adhere to strong governance principles:

- Transparency & explainability: Every AI alert must be auditable.
- Data security: Ensuring sensitive financial and personnel data remain protected.
- Bias-free Algorithms: Models trained on balanced datasets to avoid false positives.
- Continuous Learning: Feedback loops from forensic reviews to improve model accuracy.

8. The Way Forward

Indian Railways' move towards AI-enabled financial oversight will mark a transformative step in strengthening governance. Pilot projects integrating anomaly detection and predictive scoring across IPAS, IREPS, HRMS, TAMS and e-MB can lead to an institutionalized AI-based Financial Vigilance Platform.

Currently, much of the analytical work in the Indian Railways is manual. However, if structured data access is extended to stakeholders who possess domain knowledge and aptitude for AI tools, they can develop customized, stakeholder-specific AI dashboards and analytical applications.These innovations, once validated and standardized, can be adopted by CRIS for system-wide implementation across Indian Railways, ensuring uniformity and scalability.

This democratization of data access – within clearly defined security and role-based frameworks – will empower Accounts & FinanceOfficers, Auditors, and Vigilance Officers to develop their own AI-based monitoring solutions, leading to faster detection, richer insights, and greater accountability.
By blending forensic expertise with intelligent analytics, Indian Railways can achieve proactive detection, quicker intervention, and data-driven decision-making – advancing its vision of transparency, accountability, efficiency, and ethical digital governance.

.....

Disclaimer: Views expressed are personal and do not reflect the official policy/ position of the Institute.

SPECIAL FOCUS

POTENTIAL AREAS OF USE OF ARTIFICIAL INTELLIGENCE IN INDIAN RAILWAY HEALTH SERVICES

- BY DR. ARUNANGSHU SARKAR,IRHS, SR.PROF. HEALTH MGMT &
DR. S.P. CHAUDHRY, IRHS, PROF. HEALTH MGMT, IRIFM



Artificial Intelligence can transform the Indian Railway Health Service by improving diagnostics, preventive care, administration, and emergency response. Its success, however, depends on phased implementation, reliable data, and strong clinical and ethical oversight.With careful implementation and clinician involvement, AI can help deliver equitable, efficient, and data-driven healthcare to millions of railway beneficiaries.

Introduction

The Indian Railway Health Service (IRHS) provides comprehensive healthcare to nearly 7 million beneficiaries, including 1.2 million serving employees, registered retired staff, and their dependents. Its functions extend from curative and preventive healthcare to industrial health, first aid to passengers, and rapid medical response during railway disasters.

Despite sustained efforts to maintain quality, challenges persist including shortage of medical officers and paramedical staff, infrastructure constraints, and wide geographical dispersion across over 7500 stations.

Artificial Intelligence (AI), already making significant strides in healthcare, offers immense potential to enhance the reach, quality, and efficiency of IRHS. It can assist in clinical decision-making, streamline administration, improve preventive and occupational health, and optimize emergency response.

1. Diagnostics and Treatment

AI can support clinicians by enabling faster, more accurate diagnosis and treatment planning, especially in centres lacking specialist presence.

- Radiology & Pathology Interpretation: Automated reading of X-rays, CT scans, and histopathology slides can help detect abnormalities where radiologists or pathologists are unavailable.
- ECG Screening: AI-based arrhythmia(1) or ischemia(2) detection can trigger immediate alerts for specialist review or patient transfer.
- Triage: Intelligent triage tools can assess and prioritize incoming patients in emergencies, reducing waiting times and improving outcomes.
- Clinical Assistance: AI can flag deviations from treatment guidelines, alert about drug interactions, allergies, or renal dosing errors, and promote adherence to hospital antibiotic policies.
- Prediction of Deterioration: Continuous analysis of vitals and investigation data can help predict sepsis, cardiac arrest, or other deterioration early, prompting timely intervention.
- Telemedicine Augmentation: AI can assist in pre-screening patients and interpreting images or point-of-care data in sub-divisional and remote health units, strengthening specialist consultations.

Through such applications, AI can act as an “expert extender,” ensuring standardized care and early detection across the large, decentralized IRHS system.

(1)– Arrythmia - Irregular heartbeats that can be an indication of serious heart disease and sometimes may lead to sudden death

(2) – Ischaemia - Low oxygen due to inadequate blood circulation most often caused by narrowing of arteries and may lead to serious conditions like heart attacks or cerebral (brain) stroke.

2. Industrial Health

IRHS plays a critical role in occupational health and safety, where AI can greatly enhance preventive and monitoring functions.

- Predictive Occupational Risk Models: By analyzing job profiles and injury data, AI can identify high-risk activities (e.g., exposure to noise, vibration, mechanical strain) and recommend preventive measures like ergonomic interventions, job rotation, or targeted safety training.
- Injury Prediction and Safety Analytics: Integration of CCTV and sensor data can identify unsafe behaviors or conditions in workshops, sheds, and train operations, helping predict and prevent accidents.
- Medical Examination (ME): Periodic Medical Examinations are vital for operational safety. AI can compare historical and current medical data to highlight deviations that could affect fitness for duty, improving consistency and objectivity in assessments.

3. Preventive Healthcare

AI can strengthen preventive and population health programs by enabling early detection and personalized health management.

- Automated Screening: AI analysis of screening tests (audiometry, spirometry, BP, glucose) can flag early signs of disease or occupational exposure.
- Lifestyle and Chronic Disease Management: Digital therapeutics powered by AI can provide personalized guidance for diabetes, hypertension, smoking cessation, and mental health, improving adherence and outcomes.
- Vaccination Coverage and Analytics: AI can identify populations with low vaccination rates, optimize mobile immunization schedules, and improve public health planning.

Preventive health interventions reduce disease burden, absenteeism, and long-term costs, contributing to a healthier and more productive workforce.

4. Emergency Response

AI can transform disaster preparedness and response – crucial for a transport system where mass casualty incidents can occur.

- Mass Casualty Triage: AI tools can prioritize casualties using field-collected photos and vitals and recommend distribution across hospitals based on real-time capacity.
- Ambulance Routing: Integration of live traffic data, hospital load, and patient condition can guide ambulances to the best available facility.
- Automated Incident Detection: Analytics from train telemetry and CCTV can detect derailments or on-track incidents early, enabling faster dispatch of healthcare teams.

Such systems improve coordination, reduce response time, and ultimately save lives during railway accidents.

5. Healthcare Administration

AI can streamline multiple administrative and operational processes across the extensive railway healthcare network.

- **Patient Flow and Queue Management:** AI-based scheduling models can reduce waiting times and optimize outpatient operations.
- **Bed Management and Forecasting:** Predictive models can anticipate occupancy trends and manage surges during outbreaks or disasters.

- **Theatre and Staff Scheduling: Machine learning can forecast surgery durations, balance workloads, and minimize cancellations.**
- **Inventory and Pharmacy Management:** AI forecasting of medicine demand can prevent stockouts and wastage by aligning procurement with utilization patterns.
- **Predictive Equipment Maintenance:** Device telemetry can be analyzed to predict failures and schedule preventive maintenance, avoiding downtime.
- **Electronic Medical Records (EMR):** Natural Language Processing can transcribe clinician voice inputs, extract diagnoses and procedures, and automatically code them, reducing administrative load.
- **Record Linkage and Data Harmonization:** AI-enabled entity resolution can unify fragmented records from various hospitals, creating longitudinal patient histories.

Such applications increase transparency, improve utilization of resources, and ensure data-driven management across the system.

6. Training and Capacity Building

AI can also play a pivotal role in training and upskilling healthcare staff.

- **Virtual Patient Simulators:** AI-driven simulators can recreate emergency and rare clinical scenarios, helping clinicians practice decision-making safely.
- **Personalized Learning:** Adaptive platforms can tailor learning content to individual strengths and learning pace.
- **Knowledge Retrieval Assistants:** NLP-based tools can instantly fetch relevant IRHS protocols, clinical guidelines, or standard operating procedures during patient care.

AI-based training can thus help standardize knowledge and enhance competence across a geographically dispersed workforce.

AI Utilization – Benefits to IRHS

1. Enables equitable quality of care across resource-limited hospitals and remote health units.
2. Amplifies the effectiveness of telemedicine through intelligent triage and pre-assessment.
3. Enhances occupational safety through data-driven risk prediction and early health assessment.
4. Strengthens emergency response with faster, more coordinated action.
5. Reduces costs and inefficiencies across logistics, staffing, and supply chains.
6. Frees clinician time, reduces documentation errors, and supports data-driven decisions.
7. Improves continuous learning and professional development through AI-assisted training.

Important Considerations

To realize these benefits, several foundational issues must be addressed:

- **Access to Information:** AI depends on comprehensive, reliable data. While national medical guidelines (ICMR, MoHFW) provide reference data, IRHS-specific records remain incomplete. Legacy medical, occupational, and inventory data must be digitized and standardized for AI to yield meaningful insights.
- **Financial Implications:** Implementing AI across the vast IR network will involve significant costs. Pilot projects in limited divisions–such as radiology or telemedicine–should precede full-scale rollout, with clear evaluation metrics.

- **Privacy and Confidentiality:** Health data are sensitive; robust data protection and governance frameworks are essential to prevent misuse or unauthorized access.
- **Errors and Limitations:** AI models can produce inaccuracies due to limited or biased data. AI advantage depends on quick collation and integration of a great deal of information which will be almost impossible for any one person to access readily. However, AI cannot be a substitute for personal clinical evaluation of the patient by the clinician and consideration of all modifying physiological, psychological and social factors which will be different for each patient and is likely to impact the course of treatment. Thus, access to a great deal of relevant information alone can never be a substitute for wisdom and intuition gained through years of clinical experience. Clinical oversight therefore remains indispensable, and liability for errors also lies with the medical professionals. AI should therefore serve as an assistant, not a replacement, for human expertise.

Recommendations

- Start with high-value, low-risk pilots such as diagnostic imaging or telemedicine augmentation.
- Prioritize data standardization and digitization to ensure reliable inputs for AI systems.
- Maintain clinician involvement at every stage to preserve accountability and clinical judgment.
- Implement continuous monitoring and auditing of AI performance with mechanisms for retraining models.
- Uphold privacy, transparency, and fairness to build trust among users and patients.
- Invest in human capacity through training on AI tools, data handling, and change management.

Conclusion

- Artificial Intelligence offers the Indian Railway Health Service an unprecedented opportunity to strengthen diagnostic accuracy, improve preventive and occupational health, streamline operations, and enhance emergency response – all while optimizing costs across its vast network.
- Success will depend on a thoughtful, phased approach: beginning with data digitization, implementing well-defined pilot projects, measuring outcomes rigorously, and scaling proven successes under strong governance. With clinician engagement and ethical data practices, IRHS can evolve into a national model for AI-enabled, equitable, and efficient healthcare, setting a benchmark for other large public sector systems.

.....

When we talk about AI and its prospective uses, it is imperative that the thought is given to its hidden environmental impact. 'Data centres' consumer enormous amount of water for cooling; hardware becoming obsolete very fast poses questions on its disposal. Judicious use of AI is therefore important.

Scheduling computing tasks in off-peak hours, selecting energy-efficient hardware and using simple AI queries are some simple measures which can make a difference.

Use AI when truly needed, rather than by default. Informed choices will help in long-run sustainability.

Disclaimer: Views expressed are personal and do not reflect the official policy/ position of the Institute.

RAILWAY NEWS ROUND UP



Indian Railways to Sign MoU with Navigation App Mappls: Vaishnaw

DISRUPTION: STARTUPS & TECH ▸▸ 8

Indian Railways to Sign MoU with Navigation App Mappls: Vaishnaw

IT minister lauds homegrown navigation app's tech amid Swadeshi push

Our Bureau

New Delhi: Indian Railways will soon sign a Memorandum of Understanding with Google Maps competitor MapmyIndia for its homegrown navigation app Mappls, railways, and electronics & IT minister Ashwini Vaishnaw has said. Mappls technology will have various applications for the railways and the MoU, officials said on Sunday.

On Saturday, Vaishnaw experienced Mappls' features first-hand. In particular, he pointed out the apps ability to provide 3d dimensional junction views or previews of flyovers, underpasses, and roundabouts and real time driving alerts for speed limits, accident blackspots, sharp curves, speed breakers ahead, traffic signals & CCTV camera locations.

It also enables users to calculate the cost of trips, by flagging the cost of fuel and toll for specific journeys, suggesting savings with the Fastag Annual Pass brought out by the National Highway Authority of India, or based on vehicle and fuel types. Designed and developed in India, for Indian locations, it also helps users stay within speed limits and avoid risky patches.

EASING WAY

Vaishnaw highlights Mappls' ability to provide 3D previews of flyovers, underpasses as well as roundabouts



EVENTS AT IRIFM

Campus-I

- CTI Appreciation Course for IRPFS Probationers
- Forensic Accounting, Corporate and Government Accounting & Finance for SAG/SG/JAG level Accounts officers of IR.
- Senior Professional Course for CMDs & PCMDs of IR.
- Course on "Procurement Process" for IRMS(Accounts) Probationers.

Campus-II

- Training on HRMS Module (Phase-II) for Supervisory Staff of IR
- Refresher course for Supervisors Staff of Accounts Departments in IR

IRIFM Webinars:

- **Recent changes in Works Programme processing** by Shri Nimje G.C, Dy.CE/P&D/SCR
- **GST 2.0-Impact on Indian Railways** by Shri D. Krishna Kumar, AFA/Stores/SCR
- **Misclassification in Accounting system** by Shri K.Damodara Prasad, Consultant Faculty/IRIFM
- **Role of executive in processing arbitration cases in Railway contracts** by Shri K.Subramonia Pillai, Ex-FA&CAO/SR

EVENTS AT IRIFM

Commemorating the birth anniversary of Sardar Vallabhbhai Patel on 31st October 2025, all the officers, trainees and staff of IRIFM took the Rashtriya Ekta Diwas (National Unity Day) Pledge.





.....



Forensic Accounting, Corporate and Government Accounting & Finance for SAG/SG/JAG level Accounts officers of IR.

.....



Senior Professional Course for CMDs & PCMDs of IR.

NAVIGATING THE NEXT DISRUPTION: QUANTUM COMPUTING

- BY K SITHARAMARAJU, IRAS
DEAN CUM SR. PROFESSOR/IRIFM



Quantum computing is set to redefine digital power but poses major cybersecurity risks. Its ability to break current encryption threatens sensitive data and critical railway systems. The article emphases that the Ministry of Railways must act–by auditing systems, adopting post-quantum encryption, and ensuring vendor readiness. Aligned with the National Quantum Mission, these steps will secure India's digital infrastructure in the quantum era.

As public servants, we are navigating a period of unprecedented changes in digital technologies. The rapid advancement of artificial intelligence, exemplified by applications such as ChatGPT, Gemini, CoPilot, Perplexity, and DeepSeek, have transformed both global geopolitics and organisational operations. These technologies now make complex cognitive tasks, including content creation, customer support, and data analysis, widely accessible as on-demand digital solutions.

Organisations worldwide, including government agencies, are integrating these tools to enhance efficiency and foster innovation, while simultaneously establishing safeguards for data privacy and digital sovereignty.

Within the Ministry of Railways, experimental AI applications include accident prevention through driver fatigue monitoring, trespassing animal detection, predictive maintenance, and enhanced vehicle control through Kavach adaptation. Future applications may improve user experiences and also address traffic management during emergencies and disasters.

As we adopt more advanced digital intelligence, our dependence on digital infrastructure is increasing rapidly. Simultaneously, quantum computing is emerging as a disruptive technology with the potential to fundamentally redefine power and security, presenting significant challenges to the digital systems on which we depend.

What is Quantum Computing? A New Paradigm of Power

To understand the magnitude of the coming shift, we must first recognise the limitations of the computers that power our networks today. Classical computers, ranging from office desktops to central servers, process information using bits. A bit is a simple electronic switch that represents either a 0 or a 1. The complexity of modern software, including logistics, ticketing, and financial systems, is built upon billions of these binary choices. This approach is linear, solving problems one path at a time.

As mathematician Hannah Fry explains, think of solving a maze: a traditional computer tries one path at a time; a quantum computer explores all the possibilities simultaneously.

Quantum computing introduces a new fundamental unit: the qubit. Unlike a bit, which is either 0 or 1, a qubit can exist in a state of superposition, meaning it can be both 0 and 1 simultaneously. This property enables a quantum computer to explore a vast number of potential outcomes simultaneously, significantly expanding computational possibilities.

Qubits can also be linked through a quantum phenomenon known as entanglement. When two qubits are entangled, measuring the state of one instantly determines the state of the other, regardless of the physical distance between them. This property enables new forms of information processing and communication.

The combination of superposition and entanglement causes a quantum computer's power to grow exponentially with each additional qubit. While classical computers increase in power linearly, each new qubit doubles the computational space of a quantum machine. This exponential scaling enables quantum computers to solve certain problems that are currently infeasible for even the most powerful classical supercomputers.

It has the potential to transform industries from medicine to finance and AI.

The Quantum Threat: A Cryptographic Apocalypse for Critical Infrastructure[1]

This unprecedented computational power poses a direct, existential threat to our current security infrastructure. For decades, we have safeguarded our most sensitive digital assets using public-key cryptography. This foundation of modern security protects secure websites (HTTPS), digital signatures on official documents, encrypted communications for freight operations, and financial transactions within our organisation.

The security of this cryptographic framework depends on the extreme difficulty of specific mathematical problems, particularly the factorisation of huge numbers. For classical computers, factoring a 2048-bit number–a standard encryption benchmark–would require billions of years. This computational intractability underpins our digital security.

In 1994, mathematician Peter Shor developed a quantum algorithm capable of solving this problem in hours or minutes on a sufficiently powerful quantum computer. The creation of such a "cryptographically relevant quantum computer" would not simply weaken our encryption but would render it obsolete. This scenario, often termed the "Quantum Apocalypse," is considered inevitable.

The most immediate and insidious aspect of this threat is the **"Harvest Now, Decrypt Later" (HNDL) strategy.** State-sponsored actors and sophisticated criminal organisations are likely capturing and storing large volumes of our encrypted data today. This data, which includes sensitive operational commands, strategic infrastructure plans, employee payroll information, and passenger records, remains secure for now. However, these adversaries are waiting for the advent of a capable quantum computer to access this historical data. Once a quantum breakthrough is announced, it will be too late to protect these secrets.

Ramifications for the Ministry of Railways

For Indian Railways, these risks pose a direct threat to our core mission of delivering safe, efficient, and reliable transportation.

1. Operational Paralysis and Safety Risks: The command-and-control systems for our extensive rail network, including traffic management and signalling, depend on secure communications. If this encryption is compromised, adversaries could impersonate legitimate operators, alter commands to disrupt services, create scheduling chaos, or cause accidents. A Denial-of-Service (DoS) attack could immobilise our traffic management systems, halting network operations.

2. Loss of Data Confidentiality: The Ministry manages vast amounts of data, including decades of passenger records, sensitive freight manifests, internal financial deliberations, procurement contracts, and personal employee information. A quantum attack would eliminate the confidentiality of this data, eroding both the privacy we guarantee to citizens and the secrecy essential for effective operations.

[1]As per the National Critical Information Infrastructure Protection Centre (NCIIPC), “critical infrastructure” refers to systems and assets –physical or virtual– that are vital to the country’s security, economy, public health, or safety, and whose disruption can have a debilitating impact.

3. Collapse of Financial and Audit Integrity: The work of finance officers and auditors depends on trust in digital records. Digital signatures verify the authenticity of transactions, e-tenders, and audit logs, providing non-repudiation and accountability. In a post-quantum environment where digital signatures can be forged, the reliability of digital audit trails is undermined. Trust in revenue and expenditure records would be fundamentally compromised.

4. Disruption of Public-Facing Services: Ticketing systems, freight booking platforms, and passenger information services all rely on encryption for security. A quantum attack could compromise these systems, resulting in operational chaos, revenue loss, and a significant decline in public trust in Indian Railways.

India's National Response and Our Ministry's Path Forward

The Government of India has recognised this threat and is taking proactive steps. The National Quantum Mission, backed by a ₹6,000 crore budget, is spearheading our nation's efforts to become a global leader in quantum technologies. This includes developing satellite-based secure quantum communications and creating indigenous quantum-safe encryption algorithms. The Ministry of Electronics and Information Technology (MeitY) and CERT-In have jointly released a whitepaper, "Transitioning to Quantum Cyber Readiness," urging all organisations, especially those in critical sectors, to prepare for this shift.

As a Ministry, we must align with the national strategy and implement immediate, concrete actions:

1. Conduct a Comprehensive Cryptographic Inventory: We must promptly initiate a thorough audit of all systems to identify the locations and types of encryptions in use. This includes internal networks, databases, public-facing websites, and mobile applications.

2. Develop a Migration Roadmap to Post-Quantum Cryptography (PQC): We must create a strategic, phased plan to transition critical systems to emerging PQC standards. This multi-year effort will require careful planning and sustained investment.

3. Require Quantum Readiness from Vendors: Quantum readiness must become a mandatory criterion in procurement processes. All third-party vendors, including cloud service providers and software developers, should provide a clear roadmap for adopting PQC.

4. Embrace Crypto-Agility: We must develop institutional capacity to update cryptographic standards as threats evolve. This requires ongoing vigilance and adaptability, rather than a one-time solution.

The transition to a post-quantum world presents a significant challenge, but inaction is not an option. For the Ministry of Railways, this issue affects national security, economic stability, and public safety. We must approach this challenge with the same rigour and foresight used in constructing our physical infrastructure. The future security of India's railways depends on the actions we take today.

"The best way to keep something bad from happening is to see it ahead of time...
and you can't see it if you refuse to face the possibility."

.....

Disclaimer: Views expressed are personal and do not reflect the official policy/ position of the Institute.

CYBER SECURITY: STAYING VIGILANT IN THE DIGITAL ERA

- BY NIKHIL, IRMS/ACCOUNTS PROBATIONER, IRIFM



This article emphasizes the growing risk of phishing attacks targeting official railway portals like HRMS and highlights why checking website URLs before logging in is crucial for data safety. Drawing parallels between forensic investigation and cybersecurity awareness, it explains how minor lapses in digital vigilance can lead to major breaches. The article also suggests practical steps and security improvements to strengthen the cyber hygiene of Indian Railways' digital

Recently, when I opened the login page of the HRMS (Human Resource Management System) website, I encountered a pop-up message. Figure 1 displays the alert, which reads:

"Some fake HRMS sites have come to the notice of the HRMS team. All Railway Users are requested to please use URL [https://hrms.indianrail.gov.in/HRMS/] ONLY to access the valid HRMS application."

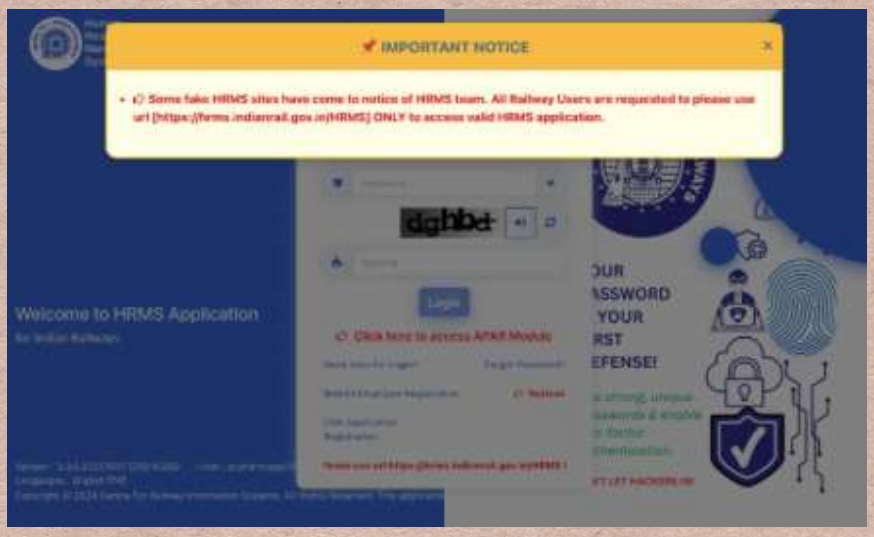


Figure 1: Pop-up on HRMS Portal

This message got me thinking- how many of us actually check the website address before entering our username and password? In one of my earlier articles, I discussed how we can perform a basic forensic analysis of financial statements. This article takes that investigative approach into the realm of cybersecurity, identifying malicious websites and ensuring safe online practices. It also offers a few observations based on my experience with portals used within the Indian Railways ecosystem.

Why Cyber Security Matters

The month of October is observed as Cyber Security Awareness Month to emphasize the importance of online safety and responsible digital behavior. The theme for this year, "Stay Safe Online," highlights the need for caution as our personal and professional lives become increasingly digitized.

As a nation, India is moving rapidly toward the vision of Digital India, and Indian Railways is embracing Industry 4.0 technologies to modernize rail transport. With this digital transformation comes the responsibility t

Cyber security isn't just about protecting servers from hackers. It's also about individual awareness because sometimes, a single careless click can compromise an entire system.

💬 ***"Amateurs hack systems; professionals hack people."***
– Bruce Schneier, Security Technologist and Author

Phishing Attacks – Don't Take the Bait!
The pop-up warning on the HRMS portal is a timely reminder of the growing threat of phishing. **Phishing** refers to the deceptive practice of creating fake websites or emails that closely resemble legitimate ones, with the intent to steal confidential information such as login credentials or financial details.

Phishing happens when fraudsters create fake websites or send deceptive emails that look exactly like official ones. Their goal is simple: trick users into revealing personal details such as passwords or OTPs.

Attackers often clone genuine websites, hosting them on different servers with slightly altered URLs to mislead users. These changes are often so subtle that at a glance, they appear authentic. The difference may be as small as one misplaced dot or letter which is easy to miss when you're in a hurry!

For instance, while the legitimate HRMS URL is:

https://hrms.indianrail.gov.in/HRMS/

some phishing variants might appear as:

https://hrms.indianrail.com/HRMS/
https://hrms.indianrail.gov.in-login.co/HRMS/
https://hrms.indianraill.gov.in/HRMS/ (extra "l")
https://hrms.indianrail.gov.in.hrmsportal.net/

These fake websites are designed to look identical to the real one, tricking users into entering their credentials. Once entered, the information is captured by the attacker, granting them unauthorized access to sensitive data.

Quick Tips to Stay Safe:
- Always type the official URL manually or use a trusted bookmark.
- Check that the site starts with https:// (the "s" stands for secure).
- Verify that it ends with .gov.in – the hallmark of an official government site.
- Never share passwords or OTPs, even with colleagues or IT staff.

"Your employees are your biggest risk–and your greatest defense."
— Theresa Payton, Former White House CIO, CEO of Fortalice Solutions

OTP or MTP?
We often rely on One-Time Passwords (OTPs) for added login security. Ideally, they should be valid once – providing a secure second step beyond your regular password. However, in portals like HRMS or Pravas, the OTP generated in the morning can be reused throughout the day. That makes it less of a One-Time Password and more of a Multiple-Time Password (MTP).

While the system remains relatively secure, this setup introduces a small window of vulnerability. If someone gains unauthorized access to your HRMS ID and daily OTP, they can continue using it for hours – until a new one is generated.

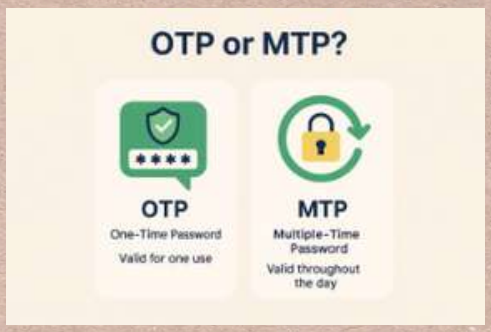


Figure 2: OTP or MTP

"An OTP should be like a disposable key – used once, and never again."

Suggestions for Safer Systems

The HRMS platform already has good security measures in place like unique HRMS IDs, passwords, and controlled access. But even small vulnerabilities deserve attention.

If a phishing attacker were to compromise the credentials of someone in a senior position, they could access sensitive employee information for an extended period. That's why periodic security reviews and stronger OTP policies are essential.

As we celebrate Cyber Security Awareness Month and strive toward a Cyber Jagrit Bharat, it's a good time to remind ourselves: cyber safety starts with us. Simple habits like verifying URLs, updating passwords, and being cautious online create the strongest defense.

Final Thoughts

Digitalization is transforming Indian Railways, making our operations smarter and more efficient. But the smarter we get, the smarter the threats become.

So next time you log in to HRMS or any other portal, pause for just a moment to check the URL, confirm the source, and stay alert. That small act of attention can protect not just your data, but the trust and integrity of our digital system.

"Cyber security isn't just an IT issue – it's everyone's responsibility."

.....

Disclaimer: Views expressed are personal and do not reflect the official policy/ position of the Institute.

CYBER SWACHH BHARAT: TOGETHER FOR A SAFER DIGITAL INDIA

- BY NEERAJ ANAND, IRPS
PROF. RELATIONS MANAGEMENT/IRIFM

The author recently attended a 3-day Special Course on Cyber Security for Officers & Supervisors dealing with CII Systems, conducted by IRISET in consultation with NCIIPC & Railway Board.

Cyber Swachh Bharat: Together for a safer Digital India

A shared mission: Cyber Swachh Bharat isn't just a government campaign–*it's a shared national responsibility*. By keeping our digital environment clean and secure, we protect not just ourselves but also the nation's journey toward a truly inclusive, trustworthy Digital India.

Every day, millions of Indians connect online–to learn, work, shop, and stay close to loved ones. The internet has become the backbone of our lives. But just like we keep our surroundings clean for good health, we must also keep our digital space clean and safe. This is the idea behind Cyber Swachh Bharat–an initiative that aims to build a secure, cyber-hygienic India where every citizen can browse, transact, and communicate on line fearlessly.

What is Cyber Swachhta Kendra?

Launched by the Ministry of Electronics and Information Technology (MeitY), the Cyber Swachhta Kendra (CSK) is India's Botnet Cleaning and Malware Analysis Centre. Its job is simple yet crucial: *to detect malicious software infecting systems, notify affected users, and help them clean their devices*. The centre works closely with internet providers, tech companies, and cyber security experts, offering free tools and practical guides to protect computers, phones, home and office networks. Free tools can be obtained from here.

Why it matters for every Indian?

Our country is embracing technology faster than ever, but with that growth comes risk. Cybercrimes are rising sharply–financial scams, phishing emails, fake apps, and identity thefts are now common. In 2024 alone, Indians lost more than ₹22,000 crore to online fraud.

A secure Digital India depends not only on government systems but also on each of us. Being cyber-aware is no longer optional–it's essential for protecting our money, identity, privacy and our work spaces.

How can we be Cyber Swachh Railway men?

Cyber safety starts with small, mindful actions–habits that keep us and our data protected:

- Use genuine, updated software instead of pirated versions.
- Think before clicking unknown links or attachments.
- Create strong, unique passwords; enable multi-factor authentication.
- Back up all important files regularly.
- Keep antivirus and security tools updated.
- Report suspicious activity on cybercrime.gov.in or call the helpline 1930.

Everyday habits for a safer online life: Stay alert when using public Wi-Fi, install apps only from official stores, and never share personal details like bank or Aadhaar information over random messages or calls. Always verify alarming alerts about "infected devices" before taking any action.

Each of these steps makes our collective cyberspace stronger.

As IR becomes more and more digitized, Back-up server and data recovery centres become very important. A safer internet begins with each of us.

.....

Disclaimer: Views expressed are personal and do not reflect the official policy/ position of the Institute.

BEST PRACTICES ON CYBER SECURITY

(In observance of October as Cyber Security Awareness Month)

1. **Use strong, unique passwords + Multi-Factor Authentication (MFA)**
   - Create passwords that are long, include a mix of upper/lower-case letters, numbers and symbols; avoid dictionary words or obvious patterns.
   - Do not use the same password for multiple accounts.
   - Wherever available, enable MFA (e.g., OTPs, authentication apps) to add an extra layer of protection.

2. **Keep software, devices and apps up-to-date**
   - Regularly install operating-system updates, security patches, and antivirus/antimalware programs – this reduces exposure to known vulnerabilities.
   - Uninstall unsupported or untrusted software/apps.

3. **Beware of phishing & suspicious links**
   - Always verify the sender, domain/URL of emails or messages before clicking links or opening attachments.
   - Be cautious of messages that urge "immediate action" or appear "too good to be true".
   - If you receive requests for credentials, OTPs or payments via links in unsolicited messages – stop, verify, report.

4. **Protect your personal & financial information**
   - Avoid sharing sensitive data (bank account numbers, passwords, Aadhaar, PAN etc.) over insecure channels.
   - Use official portals, trusted apps and check the authenticity of websites (SSL padlock, correct domain).
   - Use secure payment methods, and check for verification/transaction alerts.

5. **Use secure networks and devices**
   - Avoid using public/untrusted Wi-Fi for sensitive transactions; if necessary, use a VPN.
   - On mobile devices disable Bluetooth/NFC/GPS when not needed, and enable device-lock, encryption and "find my device" features.
   - Backup important data regularly (offline + online) so you are protected in case of malware/ransomware.

6. **Be cyber-aware and report incidents**
   - Develop cyber-hygiene habits such as logging out from shared devices, locking the screen, deleting cookies, and using unique accounts for work vs personal.
   - If you suspect a data breach, fraud or compromise, report it immediately via the designated cyber-crime portal or helpline (e.g., for India: the national portal / helpline).
   - Organizations (including public offices) should run regular awareness programmes for users, and perform periodic audits.

7. **Be mindful of digital growth & evolving threats**
   - The digital ecosystem is expanding rapidly; with it, cyber threats grow in sophistication. Stay informed about latest threats, advisories and recommended controls.
   - Use only genuine/licensed software, stay alert to botnets, malware, ransomware, and social engineering attempts.

Note: This guidance draws on official materials from CERT-In / MeitY and other Government of India sources for safe and trusted cyber practices.

- Collated by Pavan Kumar A.M.N.

The digital future belongs to the fast adopters, not the largest players.

- Klaus Schwab, Founder of the World Economic Forum

Give wings to your dreams and let them come true in 2025

IRIFM

Inspiring Excellence...

Annual Subscription

(Offline)

₹ 2400 (₹ 2000 for Railwaymen)

Single Copy: ₹ 200

Editorial Board:

Aparna Garg, DG, IRIFM

S.S. Raju, ADG, IRIFM
K. Sitharamaraju, Dean, IRIFM
Rajani Jha, PAM & Neeraj Anand, PRM
Dr. Anup N., IRAS, 2016 Batch

Secretarial Assistance:
Pavan Kumar, Manager (Conf.) & Secy. to DG/IRIFM