GOVERNMENT OF INDIA
MINISTRY OF RAILWAYS

RAJYA SABHA
UNSTARRED QUESTION NO. 1675
ANSWERED ON 13.02.2026

CURBING FRAUD IN TATKAL TICKET BOOKING

1675 SHRI PRAMOD TIWARI:

Will the Minister of RAILWAYS be pleased to state:

(a) the steps taken by Government to prevent auto-filling of forms by hacking tools and curb fraud in tatkal ticket booking;

(b) the number of accounts blocked so far; and

(c) the details of spurious attempts denied to access the e-ticketing system during the last six months?

ANSWER

MINISTER OF RAILWAYS, INFORMATION & BROADCASTING AND
ELECTRONICS & INFORMATION TECHNOLOGY

(SHRI ASHWINI VAISHNAW)

(a) to (c): The reservation ticket booking system of Indian Railways is a robust and highly secure IT platform equipped with industry-standard, state-of-the-art cyber security controls. Indian Railways has taken the following measures to prevent auto filling of forms by hacking tools and curb fraud in tatkal ticketing booking through internet and to safeguard the system from cyber attacks :

1. Aadhaar authentication to book tatkal tickets – To curb misuse and improve fairness in tatkal bookings, Aadhaar based One-Time Password (OTP) verification for online tatkal ticket booking has been introduced. Aadhaar authentication provides instantaneous verification of user uniqueness, which is critical considering the time-sensitive nature of tatkal ticket booking. It helps in preventing the creation and operation of fake or unauthorized agent-controlled multiple user account by imposing a uniqueness constraint. This measure acts as an effective safeguard against account multiplication and automated misuse, thereby ensuring fair allocation of tatkal tickets. It has contributed to improved ticket availability for genuine passengers and enhancing transparency in the online tatkal booking system.

2. Application layer Security Control -- Several application level security controls have been implemented including CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) mechanism deployed at multiple levels to avoid scripting, Brute-Force Attack and also DDoS (Distributed Denial of Service) attacks.

§

A number of security measures have also been applied for handling the OWASP (Open Web Application Security Project) for application security vulnerability.

To optimize system performance Indian Railways has implemented a Content Delivery Network (CDN) to offload static content and reduce direct traffic on internet ticket booking website system. Further, Anti-bot solutions such as AKAMAI are deployed to filter non-genuine users which help in mitigating malicious /suspicious attempts on the internet ticket booking website system and ensure smooth booking for genuine passengers. This helps in checking malicious traffic.

Use of multiple protective layers such as network firewalls, intrusion prevention systems, application delivery controllers and web application firewall to safeguard the system against cyber threats.

3. Network and Infrastructure Layer Security Controls – The entire ICT (Infrastructure & Communication Technologies) infrastructure has been deployed on high availability mode to minimize failures.

The system is protected by industry-standard state-of-the-art and data centre grade network and security equipment consisting of network firewalls, network intrusion prevention system, application delivery controllers and web application firewalls.

The system is also protected from volume-based DDoS (Distributed Denial of Service) attacks with ISP (Internet Service Provider) layer, DDoS Detection and Mitigation Services through multiple ISPs with aggregated DDoS mitigation capacity nearly 30 Gbps.

The enterprise level Content Delivery Network (CDN), anti–bot, secure DNS and Web Application Firewall (WAF) services for enhanced security, better customer experience, reducing web traffic load, resource optimisation and threat mitigation have been deployed.

For comprehensive cyber threat intelligence services, RailTel has been engaged to undertake Deep-Dark Web Monitoring, Digital Risk Protection and improve incident response.

4. Physical Security Controls – The system is hosted in a captive data center facility Chanakyapuri, New Delhi secured with CCTV footage and restricted physical access. The facility is ISO 27001 (ISMS) certified.

5. Security Audit and Monitoring -- The system is integrated with CERT-In TSAP (Threat & Situational Awareness Projects) for round the clock monitoring of security incidents and events.

§

The system has been integrated with CERT-In's "Madhu-Sanjal" wherein CERT-In has deployed the honeypot sensor for monitoring the attacker behaviors, suspicious events/intrusions attempts and learning their tactics and improve defence against cyber threats.

Security log monitoring of the system is being done by on-premises security team for detection and mitigation of security incidents.

6. Administrative measures – Several anti-fraud measures have been adopted to prevent unauthorized access and to ensure seamless booking for genuine users.

- Rigorous revalidation and verification of user accounts have been done. About 3.03 crore suspicious user IDs have been deactivated in the year 2025.
- Regular security audits of the reservation system are carried out by CERT-In empanelled information Security Audit Agencies. Moreover, internet traffic related to the ticketing system is continuously monitored by CERT-In and the National Critical Information Infrastructure Protection Centre (NCIIPC) to detect and prevent cyber attacks.
- 376 complaints have been lodged on the National Cyber Crime Portal pertaining to 3.99 lakh suspicious bookings.
- 12819 suspicious email domains have been blocked in the year 2025.

The details of spurious attempts denied to access the e-ticketing system during the last six months is as under:

December 2025	Out of 14.28 billion requests, 07.25 billion were bots.
November 2025	Out of 20.07 billion requests, 14.03 billion were bots.
October 2025	Out of 24.04 billion requests, 17.00 billion were bots.
September 2025	Out of 19.04 billion requests, 12.05 billion were bots.
August 2025	Out of 11.04 billion requests, 05.07 billion were bots.
July 2025	Out of 09.06 billion requests, 05.03 billion were bots.

*****

§