iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.81253

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

Security Risk Assessment of Major Public Transportation Hubs: Airports, Railway Stations, Bus Stands, and Metro Stations

Shashank Danaraddi, Ruchitha A (Assistant Professor)
Garden City University, India

Abstract: ***As global urbanization speeds up, major public transportation hubs, such as airports, railway stations, bus stands, and metro stations, have become essential centres of socio-economic activity. They are also high-value targets for physical and cybersecurity threats. This paper outlines a security risk assessment (SRA) framework for evaluating the specific vulnerabilities of these multimodal hubs. Airports usually have strict security measures in place, while other transit points like bus stands and railway stations often work as "open systems". This creates challenges in managing passenger flow while effectively addressing threats. The study takes a mixed-methods approach, combining Probabilistic Risk Assessment (PRA) with real-time vulnerability scanning to pinpoint critical failure points. For airports, the focus is on perimeter breaches and advanced prohibited item detection. In contrast, the assessment of metro and railway stations emphasizes crowd management and how to deal with "lone actor" or improvised explosive device (IED) threats in busy areas. The research also considers the rising risk of cyber-physical attacks on automated signalling and ticketing systems, which could disrupt the entire transit network. The findings show that the lack of consistent security cooperation across transport modes creates "security gaps" that can be exploited during intermodal transfers. The paper ends by suggesting a move toward "Resilience by Design." It supports the use of AI-driven behavioural analytics and IoT-based sensor networks to build a proactive security strategy. By transitioning from a reactive "detect-and-respond" model to a predictive intelligence-sharing framework, authorities can significantly enhance the safety of the millions of commuters who rely on these key infrastructure systems every day.***

Keywords: Security risk assessment, Urbanization, intelligence-sharing, Security gaps, Explosive device.

I. INTRODUCTION

Public transportation hubs serve as vital nodes in modern urban and intercity mobility networks, facilitating the movement of millions of passengers daily while supporting economic activity and social connectivity. Airports, railway stations, bus terminals, and metro stations share common characteristics that simultaneously enable their essential functions and create security vulnerabilities: high passenger volumes, open accessibility, complex infrastructure, and symbolic significance. These attributes make transportation hubs attractive targets for terrorist attacks and other security threats, as demonstrated by incidents in Madrid (2004), London (2005), Brussels (2016), and numerous other locations worldwide.

The security challenge facing transportation hub operators and policymakers is fundamentally one of balancing competing imperatives. Hubs must remain permeable and accessible to maintain operational efficiency and passenger throughput, yet this openness creates opportunities for adversaries. Security measures must be effective without imposing unacceptable delays, costs, or degradation of service quality. Resource constraints require prioritization among numerous potential countermeasures, necessitating systematic risk assessment methodologies that can quantify threats, vulnerabilities, and consequences while evaluating the cost-effectiveness of alternative mitigation strategies.

Transportation hubs occupy a unique position in critical infrastructure protection due to their multifaceted strategic importance. From an operational perspective, they serve as essential nodes enabling passenger mobility and freight movement, with disruptions cascading through interconnected transportation networks and broader economic systems. The concentration of passengers often numbering in the tens of thousands daily at major facilities—creates high potential for mass casualties in successful attacks. Beyond their functional role, transportation hubs carry symbolic significance as representations of modernity, connectivity, and national prestige, amplifying their attractiveness as terrorist targets.

©IJRASET: All Rights are Reserved

Intermodal facilities, where multiple transportation modes converge (e.g., rail stations at airports), present additional complexity through interdependencies that can amplify attack consequences and complicate security planning. The high visibility and media impact of attacks on transportation infrastructure serve terrorist objectives of generating fear and demonstrating capability.

This paper provides a comprehensive review of security risk assessment approaches for major public transportation hubs, examining methodologies, vulnerabilities, threats, and mitigation strategies across four hub types: airports, railway stations, bus terminals, and metro stations. The analysis synthesizes findings from 30 highly relevant scholarly sources to address critical research questions regarding frameworks, common vulnerabilities, attack vectors, and effective mitigation strategies.

II. REVIEW OF LITERATURE

A. The Strategic Importance and Threat Evolution

Transportation hubs carry symbolic significance as representations of national prestige, amplifying their attractiveness as targets. The threat spectrum has expanded from conventional explosives to chemical, biological, and radiological (CBR) agents, and more recently, cyber threats to control systems. Historical incidents like the 1995 Tokyo Sarin gas attack and the 2004 Madrid bombings have shaped modern security policy, highlighting the vulnerability of confined, high-volume spaces.

B. Vulnerability Profiles

Vulnerabilities are categorized into structural, operational, and hub-specific types.

- Airports: Focus on airside/landside separation and cargo screening.
- Metro/Rail: Face a severe throughput-versus-security trade off where comprehensive screening is often infeasible.
- Bus Terminals: Historically have the least developed security infrastructure.

III. METHODOLOGY

This study utilizes a **mixed-methods approach**.

1) Qualitative Analysis: A review of 30 scholarly sources to establish the "Resilience-by-Design" framework.
2) Quantitative/Checklist Assessment: Primary data collection from a Bengaluru transport hub (including Airport, Metro, Railway, and Bus stand areas) using a structured Risk Assessment Form.

The assessment evaluates five core domains:

- Physical & Security Risks
- Crowd & Passenger Management
- Surveillance & Monitoring
- Fire, Electrical & Structural Safety
- Cyber & Technology Risks

IV. RESULT AND DISCUSSION

The following tables summarize the findings from the Bengaluru facility audit:

1) *Physical & Security Risks*

Checklist Question	Yes	No	Remarks
Are entry and exit points controlled and monitored?	×		Biometric access used for staff entrance
Is baggage screening conducted?	×		All bags pass through X-ray scanner
Are security personnel adequately deployed?	×		Personnel stationed at all 5 main gates

2) Crowd & Passenger Management

Checklist Question	Yes	No	Remarks
Is peak-hour crowd density monitored?	×		Automated sensors track passenger inflow.
Are queue systems clearly marked?	×		Floor decals installed at ticket counters.
Are platforms and waiting areas free from congestion?		×	Congestion noted on platform 2 during 6:00 PM×

3) Surveillance & Monitoring

Checklist Question	Yes	No	Remarks
Is CCTV coverage available in all critical areas?	×		120 Cameras operational across the facility.
Are blind spots identified and rectified?		×	Corner near the north elevator needs a camera.
Is CCTV data stored securely?	×		Encrypted on-site server with 30-day backup

4) Fire, Electrical & Structural Safety

Checklist Question	Yes	No	Remarks
Are fire extinguishers accessible and inspected?	×		Last inspected February 2026
Are emergency exits clearly marked?	×		Glow-in-the-dark signage installed.
Are floors and platforms slip-resistant?	×		Non-slip coating applied to all platform edges

5) Cyber, Technology & Communication Risks

Checklist Question	Yes	No	Remarks
Is ticketing software protected from cyber threats?	×		Multi-factor authentication implemented
Are digital signboards protected from hacking?	×		Isolated from the public Wi-Fi network

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Is access to surveillance systems restricted?	×		Only authorized security leads have access.

6) Anti-Sabotage & Criminal Threats

Checklist Question	Yes	No	Remarks
Are anti-sabotage checks conducted regularly?	×		Conducted daily before the first transit cycle
Is there a bomb threat response plan?	×		Evacuation and bomb squad protocols updated.
Is coordination with intelligence/police units established?	×		Weekly briefing with local law enforcement

V. DECISION

The decision-making process in securing Bengaluru's public transport hubs must be guided by the fundamental risk equation: $Risk = Threat \times Vulnerability \times Consequence$. Based on the assessment data, the primary decision for authorities is to shift from a reactive "detect-and-respond" model to a predictive, intelligence-sharing framework.

A. Prioritizing Resource Allocation

Given the resource constraints inherent in public infrastructure, investments must be prioritized using quantitative or semi-quantitative methodologies.

- Addressing Critical Failure Points: The immediate decision must be to rectify the identified blind spot near the north elevator by installing additional CCTV coverage to ensure the facility meets the required 100% visibility standard.
- Managing High-Density Risks: Since Platform 2 exhibits significant congestion during peak hours, authorities must implement automated sensor-driven crowd management to prevent mass-casualty potential.
- Economic Optimization: Decision-makers should utilize Life-cycle Cost Analysis and Return on Investment (ROI) metrics to select countermeasures that offer the highest risk reduction per unit of expenditure.

B. Enhancing Functional Resilience

A strategic shift toward "Resilience by Design" is recommended. This involves:

- Infrastructure Hardening: Incorporating blast-resistant glazing and structural reinforcement in high-occupancy areas like waiting lounges.
- Redundancy Planning: Ensuring that critical systems—such as the encrypted on-site servers have secondary off-site backups to maintain functionality during a cyber physical attack.
- Intermodal Coordination: Establishing a unified security committee to close "security gaps" that occur during passenger transfers between the Metro, Railway, and Bus stands.

VI. CONCLUSION

The security risk assessment of major transportation hubs in Bengaluru highlights a complex environment where operational efficiency must be balanced against high-value threats. While current measures such as X-ray baggage screening, biometric staff access, and MFA protected ticketing software provide a strong baseline, the study identifies persistent vulnerabilities in crowd management and surveillance coverage.

The findings underscore that airports, while highly secure, differ fundamentally from "open systems" like bus stands and railway stations, which require more flexible, behavioural-based security layers.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

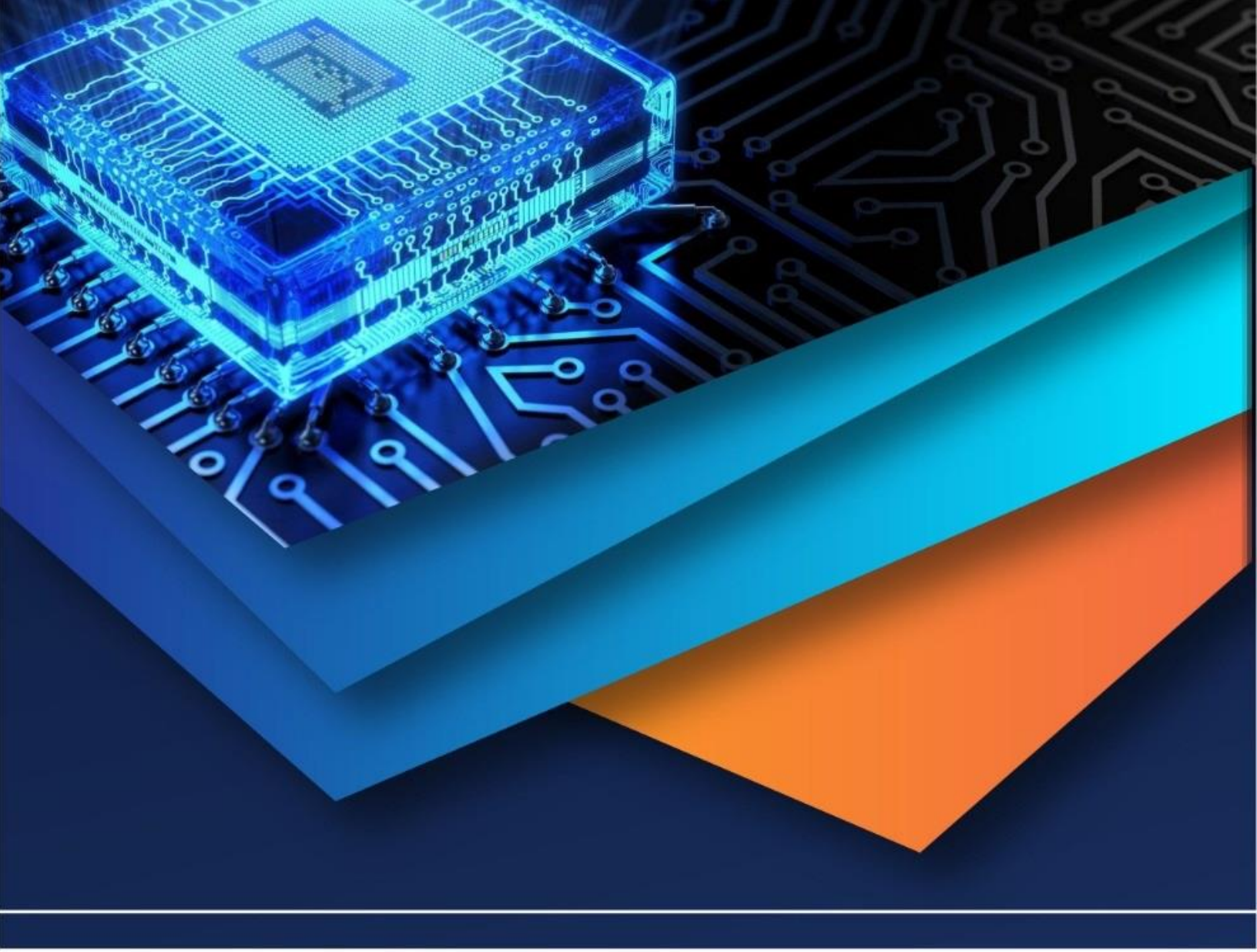
Historical precedents, such as the Madrid and London bombings, serve as a reminder that the concentration of passengers in confined or underground spaces remains a primary target for explosive and chemical threats.

Ultimately, the safety of the millions of daily commuters depends on a proactive strategy. By integrating AI-driven behavioural analytics, maintaining strict fire and electrical safety inspections, and fostering weekly coordination with local law enforcement, Bengaluru can lead the way in building a resilient urban transit network. Future efforts must focus on standardizing these assessment parameters across all transport modes to ensure no single node becomes a "weak link" in the city's critical infrastructure.

REFERENCES

[1] S. Kaewunruen, J. M. Sussman, and A. Matsika, "A Decision Framework for Managing the Risk of Terrorist Threats at Rail Stations Interconnected with Airports," Safety, vol. 4, no. 3, 2018. https://doi.org/10.3390/SAFETY4030036
[2] A. Zahrani, "Assessing and Proposing Countermeasures for Cyber-Security Attacks," International Journal of Advanced Computer Science and Applications, vol. 13, no. 1, 2022. https://doi.org/10.14569/ijacsa.2022.01301102
[3] Sanchez, J. Carpio, and J. M. Menendez, "SECURESTATION: Passenger Station and Terminal Design for Safety, Security and Resilience to Terrorist Attack," 2014.
[4] Fang, Y. Xiang, F. Xu, and L. Ma, "Risk analysis of Chongqing urban rail transit network," Journal of Loss Prevention in the Process Industries, vol. 66, 2020. https://doi.org/10.1016/J.JLP.2020.104182
[5] Katzman, "Protecting Against Terrorist Attacks for Urban Transportation Projects," WIT Transactions on the Built Environment, 2005. https://doi.org/10.2495/SAFE050731
[6] Lazarick, "Airport vulnerability assessment-a methodology evaluation," in Proc. 33rd Annual Int. Carnahan Conf. on Security Technology, pp. 103-109, 1999. https://doi.org/10.1109/CCST.1999.797904
[7] Lazarick, "Airport vulnerability assessment-an analytical approach," in Proc. 32nd Annual Int. Carnahan Conf. on Security Technology, pp. 86-93, 1998. https://doi.org/10.1109/CCST.1998.723763
[8] D. Lazarick, "Airport vulnerability assessment: an analytical approach," Proc. SPIE, vol. 3575, pp. 92-101, 1998. https://doi.org/10.1117/12.334999
[9] Matsika, S. O'Neill, U. Battista, M. Khosravi, A. Laporte, and E. Munoz, "Development of Risk Assessment Specifications for Analysing Terrorist Attacks Vulnerability on Metro and Light Rail Systems," Transportation Research Procedia, vol. 14, pp. 1345-1354, 2016. https://doi.org/10.1016/J.TRPRO.2016.05.207
[10] E. Soehnchen, M. Bürger, and M. Maly, "A Risk Assessment Tool for Public Transport," 2014.
[11] Flammini, N. Mazzocca, and V. Vittorini, "Quantitative Security Risk Assessment and Management for Railway Transportation Infrastructures," in Critical Information Infrastructures Security, Lecture Notes in Computer Science, vol. 5508, pp. 180-189, 2009. https://doi.org/10.1007/978-3-642-03552-4_16
[12] Fiumara, "The Railway Security: Methodologies and Instruments for Protecting a Critical Infrastructure," in Handbook of RAMS in Railway Systems, pp. 35-49, 2015. https://doi.org/10.1007/978-3-319-04426-2_3
[13] G. Tamasi and M. Demichela, "Risk assessment techniques for civil aviation security," Reliability Engineering & System Safety, vol. 96, no. 8, pp. 892-899, 2011. https://doi.org/10.1016/J.RESS.2011.03.009
[14] Alawad, S. Kaewunruen, and J. M. Sussman, "Complex-system decision framework for managing risks to rail stations at airports from terrorist threats," in Proc. 5th Int. Conf. Road and Rail Infrastructure (CETRA), 2018. https://doi.org/10.5592/CO/CETRA.2018.665
[15] Kolesár, M. Kelemen, and V. Blišťan, "Safety Management System Protection against Acts of Unlawfull Interference of Civil Airport," 2012.
[16] M. Wilson, B. A. Jackson, M. Eisman, P. Steinberg, and K. R. Riley, "Securing America's Passenger Rail Systems," RAND Corporation, 2008.
[17] O. Avci, K. Bhargava, D. H. Tobias, and M. Bittner, "Threat and vulnerability risk assessment for existing subway stations: A simplified approach," Case Studies on Transport Policy, vol. 6, no. 4, pp. 663-673, 2018. https://doi.org/10.1016/J.CSTP.2018.08.005
[18] S. Starita, M. P. Scaparra, and J. R. O'Hanley, "Assessing Urban Rail Transit Systems Vulnerability: Metrics vs. Interdiction Models," in Critical Information Infrastructures Security, Lecture Notes in Computer Science, vol. 11260, pp. 144-155, 2017. https://doi.org/10.1007/978-3-319-99843-5_13
[19] T. Szatmári, M. Hovanec, and J. Mašek, "Vulnerability assessment and risk prioritization with HRVA method for railway stations," Transportation Research Procedia, vol. 55, pp. 1179-1186, 2021. https://doi.org/10.1016/J.TRPRO.2021.07.155
[20] V. Recagno, A. Hernandez, and R. Faller, "SARA: Tool to Assess and Improve Functional Resilience from Security Attacks of Passenger Intermodal Stations and Terminals," 2015.
[21] Y. M. Alostaz, "TVRA and Application to a Transit Center: A Case History Study," in Proc. Structures Congress 2023, pp. 28-39, 2023. https://doi.org/10.1061/9780784484777.004

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)