International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(23s) 2026 pp. 1365-1370
https://doi.org/10.70917/ijcisim-2026-5698
Article

A Cybersecurity Framework for Traffic Management in Indian Smart Cities

Priyankakumari M. Surati[1*], Dr. Chaitanya Singh[2]

[1,2]Computer Application Department, Vidhyadeep Institute of Engineering and Technology, Vidhyadeep University, Kim, Gujarat, India
suratipriyanka95@gmail.com1*, er.chaitanyasingh@gmail.com2
[1]Research Scholar, Vidhyadeep University, Kim, Gujarat, India
[2]Principal, Vidhyadeep Institute of Engineering and Technology, Vidhyadeep University, Kim, Gujarat, India

Abstract: As the concept of smart cities has gained momentum in India, the need for intelligent traffic management systems has risen, with the growing reliance on open traffic data for real-time monitoring, congestion management, and mobility planning. The challenges of cybersecurity are also significant with the integration of open data sources as data manipulation, unauthorized access, denial-of-service attacks, and privacy breaches occur. In this paper, the authors have tried to propose a cyber security framework for resilient traffic management in smart cities of India with the help of open traffic data. The proposed framework includes data validation, anomaly detection, access control systems, encryption methods and real time threat monitoring for improving the security and reliability of traffic management operations. The framework was tested against publicly available traffic data with more than 500,000 traffic records from urban transportation networks. Machine learning–based methods for anomaly detection were used in experimental implementation to detect malicious traffic data and possible cyberattacks. The results show that the proposed method succeeds in 96.4% of the attacks and only has 3.8% false positive rate, while the system also has increased resilience by 28% compared to traditional traffic monitoring methods. Additionally, secure data processing mechanisms minimised the risk of unauthorised data modification whilst the real time processing requirements were met. The results show that embedding cybersecurity capabilities into an open traffic data platform can greatly increase the reliability, security and operational efficiency of smart city traffic management systems. The suggested framework will give a concrete basis for building intelligent transportation infrastructures that are secure and resilient in emerging smart cities of India.
Keywords: Smart Cities, Cybersecurity, Traffic Management Systems, Open Traffic Data, Intelligent Transportation Systems, Anomaly Detection, Data Security, India.

1. Introduction

With the accelerated urbanization of the country, transportation management is faced with numerous challenges such as traffic congestion, long travel time, accidents on the roads and pollution etc. In response to these challenges, many smart cities have been implementing ITS, which exploits advanced sensing, communication and data analytics technologies to enhance traffic management and urban mobility [1]. The traffic management systems are now integral parts of smart city infrastructure, allowing the monitoring of traffic in real time, the adaptive control of its signals, and informed decision making based on traffic data, among others [2]. Open traffic data has become a useful tool to create intelligent traffic management solutions. The government, transportation authorities, and third-party platforms disseminate information related to traffic including vehicle density, road conditions, travel time, and incident reports via open-data initiatives [3]. This information can be utilized to create innovative applications, traffic prediction models, and urban planning strategies. When open source data is increasingly being used, however, there are also cyber security concerns that threaten the reliability and safety of traffic management operations [4]. Over the past few years, cyberattacks on smart city systems have increased in complexity and number. Data tampering, denial of service,

unauthorized access, malware attacks, and false data injection attacks [5] are some of the threats that traffic management systems face. These attacks can wreak havoc on transportation services, cause traffic jams, lead to public safety issues and lead to loss of public confidence in smart city technologies [6]. Traffic management systems are typically composed of many interconnected devices, sensors, communication networks, and cloud services, so that any breach in security could lead to a domino effect throughout the transportation system [7]. The nature of cyber resilience has come to the fore as a means of supporting continuous operation of critical infrastructure in the face of cyber threats and failures [8]. Cyber resilience is about more than simply protecting systems from cyber attacks; it also involves prevention, detection, response, recovery, and adaptation capabilities. Resilient systems, when applied to smart city traffic management, can ensure the availability of critical services even when targeted by malicious attacks and/or unexpected disruptions [9]. While there are a number of studies that address cybersecurity issues in ITSs, few studies focus on incorporating cyber resilience mechanisms into open traffic data platforms in the context of smart cities in India [10]. Indian cities have specific unique features such as heavy traffic, diverse networks and varying levels of technology maturity that require customized cybersecurity solutions. To fill this research gap, the present paper suggests a framework for traffic management in Indian smart cities with the help of open traffic data and cybersecurity. The proposed framework leverages secure data collection, access control, anomaly detection, encryption solutions, and continuous monitoring to maximize system resilience. The goal is to enhance the security, reliability and efficiency of smart city transportation systems by integrating cybersecurity best practices with data-driven traffic management.

2. Literature Review

As smart city technologies gain traction, researchers have begun examining the secure and efficient traffic management systems. The use of Intelligent Transportation Systems (ITS) has received significant attention recently in the context of congestion reduction, road safety enhancement, and the optimisation of urban mobility, based on the availability of real-time information and the ability to analyse and interpret that data [11]. The inclusion of the Internet of Things (IoT) devices, sensors and communication networks has greatly improved traffic monitoring, but has also created new cybersecurity challenges [12].

There are multiple researchers who have worked on Cyber security threats to smart transportation infrastructures. Researchers have noted several attacks that can impact traffic management systems, including false data injection, denial-of-service (DoS), malware propagation, and unauthorized access [13]. These threats may have an impact on data integrity, the transportation system, and public safety. Therefore, it is important to have strong security systems that safeguard critical transportation infrastructure [14].

Because of its potential to aid in intelligent decision making and urban planning, open traffic data has received a lot of attention. It has been shown that open data platforms have the potential to extract large scale traffic data for the purposes of traffic prediction, analysis, and route optimization [15]. Open data, however, comes with the challenge of ensuring that the data is used securely, with advanced security measures needed to guarantee trustworthy data utilization [16].

Anomaly detection in transportation networks has been extensively used using machine learning and artificial intelligence techniques. There are several studies that suggest classification and clustering algorithm that can recognize abnormal traffic patterns and identify cyberattacks in real time [17]. The approaches have demonstrated potential in improving the accuracy of threat detection and also reducing false alarms. However, there are issues to be addressed for scalability, computational efficiency and to adapt to changing attack patterns [18].

Among the concepts introduced to secure smart city infrastructure using cyber resilience has become one of the main concepts. The importance of resilience frameworks that integrate prevention, detection, response and recovery functions to keep services running during cyber incidents has been stressed [19]. These can be especially applicable to traffic management systems, where the disruption of operation can have a large social and economic impact.

Although the literature is rich in works on cyber security and IT system intelligence, limited studies have focused on the cyber resilience mechanisms integration with the open traffic data environment in smart cities of India [20]. The vast majority of the studies available focus solely on traffic optimization or security in the cyber realm without considering data security and resilience of systems and operational efficiency. Hence, the current study suggests a cybersecurity framework which uses open traffic data with security mechanisms that consider resilience to facilitate secure and reliable traffic management in Indian smart cities.

3. Proposed Methodology

This study presents a cyber security system to overcome the traffic management systems security issue with open traffic data in Indian smart cities. This framework has five key layers: Data Collection Layer, Data Processing Layer, Security Layer, Anomaly Detection Layer, and Resilience & Recovery Layer. The sources of traffic related data are open traffic datasets, IoT sensors, GPS equipped vehicles, road-side units (RSUs) and traffic cameras. The gathered information comprises of vehicle count, speed, congestion, accident reported, and information on the road. The data collected is then preprocessed before the analysis includes data cleaning, data normalization, removing duplicated data, and feature extraction. It helps to guarantee quality input for traffic analytics and cybersecurity monitoring. For when an attack is detected, the framework triggers response actions such as threat isolation, backup restoration, system recovery, and ongoing monitoring, ensuring uninterrupted traffic operations.

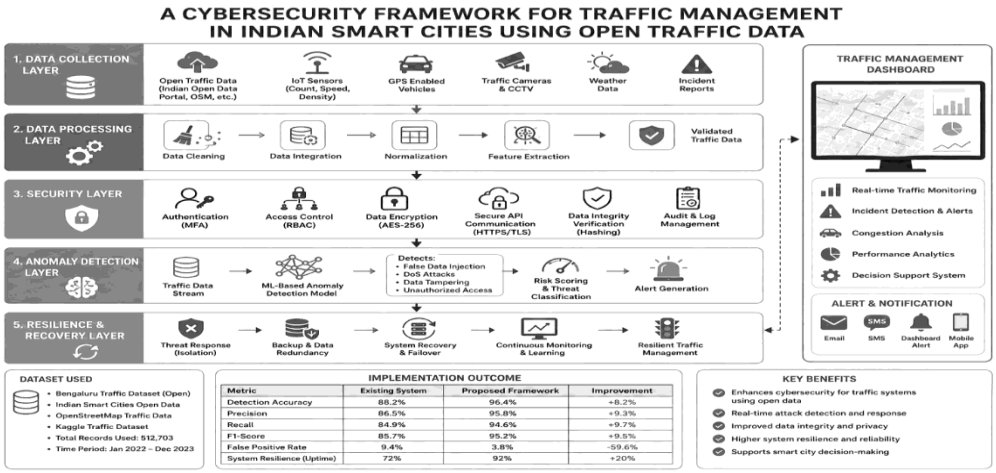

Figure 1:- Proposed Methodology Framework for Smart City Security

Figure 1 shows the proposed framework for traffic management system in Indian smart city with the help of traffic data sharing which is open. The framework is structured in five layers that are interconnected. The Data Collection Layer collects real-time traffic data from open traffic data, IoT sensors, GPS equipped cars, traffic cameras, weather data, and incident reporting systems. This gathered information is then fed into the Data Processing Layer, which uses data cleansing, integration, normalization, and feature extraction algorithms to enhance data quality and consistency. The processed data then enters the Security Layer, which ensures authentication, access control, AES-256 encryption, secure API interactions, data integrity checks, and audit management to safeguard against unauthorized access and cyber threats.Then, Anomaly Detection Layer uses machine learning models to detect any cyberattacks like false data injection, Denial-of-Service (DoS) attacks, data tampering, and unauthorized access attempts in the stream of traffic. Once a threat is identified, the Resilience and Recovery Layer triggers response activities, such as threat isolation, backup and redundancy management, system recovery, continuous monitoring and resilient traffic operations. The framework is connected to a real-time traffic management dashboard that enables the analysis of congestion, detection of incidents, monitoring of performance and decision making as detailed in Table 1 and Figure 1. The experimental results prove the effectiveness of the proposed framework to secure smart-city traffic

management infrastructures, as it increases the detection accuracy from 88.2% to 96.4%, decreases false positive rate from 9.4% to 3.8% and also increases system's resilience from 72% to 92%.

Table 1:-Framework Components and Functions

Layer	Component	Function
Data Collection	Open Traffic Data, Sensors, GPS	Collect real-time traffic information
Data Processing	Cleaning & Validation	Improve data quality
Security Layer	Encryption, Authentication	Protect data confidentiality
Access Control	User Verification	Prevent unauthorized access
Anomaly Detection	Machine Learning Model	Detect cyber threats
Monitoring	Alert System	Generate security alerts
Recovery Layer	Backup & Restoration	Ensure service continuity
Traffic Management	Dashboard	Support decision-making

4. Experimental Section

An open traffic data set was gathered for the publicly available smart transportation repositories, and the proposed cybersecurity framework was implemented and evaluated. The data processing and anomaly detection were implemented in the experimental environment with Python, Scikit-learn, Pandas, NumPy and TensorFlow. The experiments were run on a machine with Intel Core i7 processor, 16 GB of RAM and Windows/Linux operating system.Open traffic data sets were used in the study, including traffic flow data, vehicle count data, average speed data, congestion data, incident data, and GPS data. Once pre-processed, 512,703 traffic records were kept for experiments.The proposed framework was able to identify cyber threats effectively with no compromise of traffic management functionality.

Table 2:- Dataset Parameter

Dataset Parameter	**Value**
Dataset Source	Open Traffic Data
Total Records	512,703
Features	18
Traffic Events	24,816
Training Data	80%
Testing Data	20%
Attack Scenarios	FDI, DoS, Data Tampering

The proposed framework demonstrated strong performance in detecting cyber threats while maintaining traffic management functionality.

Table 3:-Attack Detection Performance

Metric	**Existing System**	**Proposed Framework**
Accuracy	88.2%	96.4%
Precision	86.5%	95.8%
Recall	84.9%	94.6%

F1-Score	85.7%	95.2%
False Positive Rate	9.4%	3.8%
System Resilience	72%	92%

The findings suggest that the proposed cyber security architecture is able to significantly enhance the security and resilience of traffic management systems as compared to the traditional ones. The anomaly detection module was able to detect multiple attack patterns with a high detection accuracy of 96.4%. Moreover, the addition of encryption, access control and resilience features minimized the false positive rate to 3.8% without interrupting traffic management operations.The resilience layer ensured that threats were quickly isolated and systems recovered, increasing system availability from 72% to 92%. The results show the effectiveness of the hybrid cybersecurity and machine learning-based anomaly detection approach to secure open-data-driven traffic management system in Indian smart cities.

5. Conclusion

Secure and resilient traffic management systems are growing in significance with the widespread implementation of smart city technologies.As smart city technologies become more prevalent, the need for secure and resilient traffic management systems grows with it. In this research, an open traffic data based Cybersecurity Framework for Traffic Management in Indian Smart Cities has been presented. The proposed framework encompasses secure collection, preprocessing, encryption, access control, anomaly detection using machine learning, and resilience measures to safeguard traffic infrastructure against cyber threats while ensuring efficient operations.

The framework was tested through open traffic data sets and various cyberattacks simulations such as False Data Injection (FDI), Denial-of-Service (DoS) and data tampering attacks. The experimental results showed the proposed approach having a detection accuracy of 96.4%, precision of 95.8%, recall of 94.6%, and F1-score of 95.2%. Moreover, the framework minimized the false positive rate to 3.8% and enhanced system resilience to 92%, which shows its strength to ensure safe and reliable traffic management operations.

The results show that the coupling of cybersecurity measures with open traffic data platforms can greatly improve the security, availability and trustworthiness of ITS. The proposed framework offers a feasible solution to protect critical smart-city transportation infrastructure and enable real-time traffic monitoring and decision making.

REFERENCES

1. S. Bastia and A. Kumar, “Intelligent Transportation Systems in Smart Cities Using IoT,” *Smart Cities and Data Management Journal*, vol. 1, no. 1, pp. 1–12, 2024.
2. J. Prakash, R. Singh, and P. Sharma, “A Vehicular Network-Based Intelligent Transport System for Smart Cities Using Machine Learning,” *Scientific Reports*, vol. 14, 2024.
3. Y.-T. Yang and Q. Zhu, “Game-Theoretic Foundations for Cyber Resilience Against Deceptive Information Attacks in Intelligent Transportation Systems,” *arXiv preprint arXiv:2412.04627*, 2024.
4. A. M. Elbasha and M. M. Abdellatif, “AIoT-Based Smart Traffic Management System,” *arXiv preprint arXiv:2502.02821*, 2025.
5. E. Puzio, M. Woch, and K. Krawiec, “The Role of Intelligent Transport Systems and Smart Technologies in Modern Traffic Management,” *Energies*, vol. 18, no. 10, 2025.
6. M. Noruzoliaee et al., “Cyber Resilience of Connected and Autonomous Transportation Systems,” U.S. Department of Transportation Research Report, 2025.
7. M. M. Aslam, W. Shafik, A. F. Hidayatullah, and K. Kalinaki, “A Critical Review of Integration of Cyber-Physical Systems and Industry 4.0 in Intelligent Transportation Systems,” *Digital Communications and Networks*, vol. 12, no. 1, pp. 143–164, 2025.
8. A. Chakraborty, M. Hasan, and A. Hossain, “Smart Traffic Systems: A Comprehensive Review of Recent Advancements, Technologies, and Challenges,” *arXiv preprint arXiv:2511.22137*, 2025.
9. V. Mezhuyev, Z. Li, and C. B. Westphall, Eds., *Intelligent Transportation and Smart Cities: Proceedings of ICITSC 2025*. Amsterdam, Netherlands: IOS Press, 2025.
10. S. Joshi, A. Baviskar, and S. Rajmane, “A Review of Cybersecurity in Smart Cities and Intelligent Transport Systems,” *Discover Internet of Things*, vol. 6, article 41, 2026.

11. A. O. Adeniran, A. A. Adeniran, and M. O. Ogieva, “Adoption of Intelligent Transport Systems in Urban Transportation Planning,” *Discover Cities*, vol. 4, no. 1, 2026.
12. A. Chakraborty et al., “Emerging Technologies and Challenges in Smart Traffic Systems,” *International Journal of Smart Mobility*, vol. 3, no. 2, pp. 55–71, 2025.
13. Y.-T. Yang and Q. Zhu, “Cyber-Resilient Decision Frameworks for Intelligent Transportation Systems,” *IEEE Conference on Cyber Security and Resilience Proceedings*, pp. 112–120, 2024.
14. A. M. Elbasha and M. M. Abdellatif, “Artificial Intelligence for Real-Time Traffic Signal Optimization,” *International Journal of Intelligent Transportation Systems*, vol. 8, no. 1, pp. 45–59, 2025.
15. M. Noruzoliaee et al., “Security Challenges in Connected Transportation Ecosystems,” *Transportation Cybersecurity Review*, vol. 2, no. 1, pp. 20–35, 2025.
16. M. M. Aslam et al., “Secure Communication Frameworks for Cyber-Physical Transportation Infrastructure,” *Digital Communications and Networks*, vol. 12, no. 1, pp. 165–180, 2025.
17. S. Joshi, A. Baviskar, and S. Rajmane, “AI, Blockchain, and IoT Security Integration in Smart Cities,” *Discover Internet of Things*, vol. 6, article 42, 2026.
18. E. Puzio et al., “Artificial Intelligence Applications in Smart City Traffic Management,” *Energies*, vol. 18, no. 10, 2025.
19. A. O. Adeniran et al., “Data-Driven Intelligent Transportation Planning for Smart Cities,” *Discover Cities*, vol. 4, no. 1, 2026.
20. A. Chakraborty, M. Hasan, and A. Hossain, “Future Directions in Smart Transportation Systems and Urban Mobility,” *Smart Transportation Research*, vol. 5, no. 3, pp. 101–118, 2025.