GYANBODH
An International Multidisciplinary Peer Reviewed Journal
ISSN:3048-9792
Volume: 3
Issue: 3
May - June: 2026

Architectural and Operational Failures in Security Logging within Ahmedabad Smart Traffic Control Framework

Amin Manishaben Arkhabhai
Ph.D. scholar, Hemchandracharya North Gujarat University, Patan

Dr. Kirit I. Chokhawala
Assistant Professor, Department of Computer and IT, HNGU, Patan

Abstract

Smart Traffic Control Systems are becoming an important part of modern smart cities. Ahmedabad has adopted intelligent traffic technologies such as CCTV cameras, adaptive traffic signals, IoT sensors and Integrated Command and Control Centres to improve traffic management and road safety. While these technologies provide many benefits, they also increase cybersecurity risks. Security logging and monitoring are essential for detecting cyber threats and maintaining reliable traffic operations. Weak logging practices or poor monitoring may allow attackers to access systems without being detected, leading to service disruption and security incidents. This paper presents an analytical study of security logging and monitoring failures in the Ahmedabad Smart Traffic Control System. The study is based on secondary data collected from research articles, cybersecurity standards, government reports and smart city publications. The findings show that fragmented log management, inadequate real-time monitoring, weak IoT security, human errors and insufficient incident response are major challenges. The paper recommends centralized log management, continuous monitoring, staff training, regular security audits and the adoption of international cybersecurity standards to improve the security and reliability of smart traffic infrastructure.

Keywords: Smart Traffic System, Security Logging, Monitoring, Cybersecurity, Ahmedabad, Smart City

1. Introduction

Smart city technologies have changed the way urban transportation is managed. Traditional traffic systems mainly depended on fixed signal timings and manual supervision, whereas modern smart traffic systems use digital technologies to improve traffic movement and road

GYANBODH
An International Multidisciplinary Peer Reviewed Journal
ISSN:3048-9792
Volume: 3
Issue: 3
May - June: 2026

safety. These systems collect information from CCTV cameras, traffic sensors, communication networks and cloud platforms to make decisions in real time.

Ahmedabad is one of the leading smart cities in India that has implemented an advanced Smart Traffic Control System. The system includes adaptive traffic signals, surveillance cameras, automatic number plate recognition (ANPR) and an Integrated Command and Control Centre (ICCC). These technologies help reduce traffic congestion, improve emergency response and support law enforcement activities.

Although digital technologies have improved traffic management, they have also created new cybersecurity challenges. Every connected device generates digital records called security logs. These logs record activities such as user logins, system updates, network communication and configuration changes. They help administrators understand what is happening inside the system and support investigations when security incidents occur.

However, generating logs alone is not enough. The logs must be monitored continuously to detect unusual activities at an early stage. If monitoring is weak, cyber attackers may remain unnoticed and could manipulate traffic systems, interrupt communication networks, or access sensitive information.

The Ahmedabad Smart Traffic Control System combines different technologies supplied by multiple vendors. This creates challenges in collecting and analysing logs from different devices. Therefore, effective security logging and monitoring are necessary to maintain reliable traffic operations and protect critical infrastructure.

This study analyses the major failures in security logging and monitoring and suggests practical measures to improve cybersecurity in the Ahmedabad Smart Traffic Control System.

2. Literature Review

Researchers have emphasized that cybersecurity is becoming increasingly important in smart city infrastructure. Modern transportation systems depend on IoT devices, cloud computing, communication networks and intelligent control systems. These technologies improve operational efficiency but also increase cybersecurity risks.

According to Stallings (2020), security logs provide important evidence for detecting cyber attacks and investigating security incidents. Proper log management helps organizations identify suspicious activities before they cause major damage.

GYANBODH
An International Multidisciplinary Peer Reviewed Journal
ISSN:3048-9792
Volume: 3
Issue: 3
May - June: 2026

The National Institute of Standards and Technology (NIST, 2022) explains that organizations should continuously collect, store, analyse and monitor security logs. Effective monitoring allows administrators to identify unauthorized access, system failures and network attacks quickly.

Recent studies also show that smart traffic systems generate large volumes of operational data every day. Manual analysis of these logs is difficult, making automated monitoring tools and Security Information and Event Management (SIEM) systems increasingly important.

Researchers have further observed that IoT devices often have limited storage and processing capacity, which affects their ability to generate detailed security logs. Cloud computing introduces additional monitoring challenges because organizations must manage both local infrastructure and cloud-based services.

Although previous studies discuss cybersecurity in smart cities, limited research specifically analyses security logging and monitoring failures in Indian smart traffic systems. This study attempts to fill that gap by focusing on Ahmedabad.

3. Research Gap and Objectives

Most existing studies discuss cybersecurity challenges in smart cities from a general perspective. Limited attention has been given to security logging and monitoring failures in smart traffic systems operating in Indian cities. There is also little research examining organizational issues such as fragmented logging, delayed monitoring and insufficient incident response.

The objectives of this study are:

- To understand the role of security logging in smart traffic systems.
- To identify major logging and monitoring failures.
- To analyse the cybersecurity risks associated with these failures.
- To suggest practical measures for improving cybersecurity in the Ahmedabad Smart Traffic Control System.

4. Research Methodology

The present study is based on a qualitative analytical research method. Secondary information has been collected from research journals, books, government publications, cybersecurity standards, Smart City Mission reports and NIST guidelines.

GYANBODH
An International Multidisciplinary Peer Reviewed Journal
ISSN:3048-9792
Volume: 3
Issue: 3
May - June: 2026

The collected information was analysed to identify common security logging and monitoring problems in smart traffic systems. The study compares existing practices with recommended cybersecurity frameworks and develops practical suggestions for improvement.

Since access to the operational data of the Ahmedabad Smart Traffic Control System is restricted, the study is based on analytical observations rather than primary field investigation.

5. Analytical Study of Security Logging and Monitoring Failures in Ahmedabad Smart Traffic Control System

Smart Traffic Control Systems represent a complex cyber-physical environment where physical infrastructure and digital technologies work together. In Ahmedabad, intelligent traffic management depends on multiple components such as CCTV surveillance systems, IoT-based sensors, adaptive traffic signals, communication networks, cloud platforms and the Integrated Command and Control Centre (ICCC). Each component continuously generates operational and security-related information. Proper collection and analysis of this information are necessary to identify cyber threats and maintain uninterrupted traffic services.

Security logging and monitoring failures can create serious vulnerabilities in such systems. A failure in detecting unusual activities may allow attackers to compromise traffic signals, manipulate collected data, or disrupt communication between different components. The following sections analyse the major security logging and monitoring challenges associated with smart traffic infrastructure.

5.1 Fragmented Log Management

One of the major challenges in smart traffic systems is the absence of a unified log management approach. Ahmedabad Smart Traffic Control System consists of different technologies provided by multiple vendors. CCTV cameras, traffic controllers, IoT sensors, network devices, databases and software applications may generate logs in different formats.

When logs are stored separately across different systems, security teams face difficulties in collecting and analysing information. An attacker who moves between different components may leave small traces in multiple locations, but these traces may not be connected during investigation.

GYANBODH
An International Multidisciplinary Peer Reviewed Journal
ISSN:3048-9792
Volume: 3
Issue: 3
May - June: 2026

For example, an unauthorized login attempt on a traffic control server and unusual communication from an IoT sensor may appear as separate events if there is no centralized monitoring system. As a result, security teams may fail to identify a coordinated cyber attack. A centralized Security Information and Event Management (SIEM) system can overcome this problem by collecting logs from different sources, correlating events and generating alerts. Without such integration, the effectiveness of security monitoring remains limited.

5.2 Inadequate Real-Time Monitoring

Modern smart traffic systems require continuous monitoring because they operate twenty-four hours a day. However, many organizations still depend on periodic reviews of system logs rather than real-time analysis.

Delayed monitoring creates opportunities for attackers to remain inside the system for longer periods. Cyber threats such as unauthorized access, malware infection, data manipulation and network attacks require immediate detection and response.

In a traffic management environment, even a short delay in identifying a security incident may affect traffic operations. For instance, manipulation of traffic signal data during peak hours can increase congestion and create safety risks.

Real-time monitoring tools using artificial intelligence and machine learning techniques can help identify abnormal patterns. These systems can analyse large volumes of data and detect unusual behaviour faster than manual methods.

5.3 Weak Security Logging Practices in IoT Devices

IoT devices are important components of smart traffic infrastructure. Sensors and connected devices collect traffic volume, vehicle movement, environmental conditions and other operational information. However, many IoT devices have limited computing capacity, which restricts their ability to maintain detailed security logs.

Common IoT logging weaknesses include:

- Limited storage capacity for maintaining historical logs.
- Lack of standard formats for security records.
- Incomplete recording of user activities.
- Difficulty in updating security features.
- Weak authentication mechanisms.

GYANBODH
An International Multidisciplinary Peer Reviewed Journal
ISSN:3048-9792
Volume: 3
Issue: 3
May - June: 2026

If IoT devices do not generate sufficient security information, administrators may find it difficult to identify the source of an attack. Additionally, compromised IoT devices can become entry points for attackers to access larger parts of the traffic network.

Therefore, IoT security design should include secure logging mechanisms, device authentication, encryption and regular firmware updates.

5.4 Lack of Effective Log Analysis and Threat Detection

Collecting logs is only the first step in cybersecurity management. The real value of logs comes from analysing them effectively. Large smart traffic systems generate huge amounts of information every day, making manual analysis almost impossible.

Without advanced analytical tools, security teams may experience:

- Difficulty in identifying abnormal behaviour.
- High numbers of false alerts.
- Delayed incident investigation.
- Failure to recognize advanced attacks.

Machine learning-based security analytics can improve threat detection by learning normal system behaviour and identifying deviations. For example, unusual login patterns, unexpected communication between devices, or sudden changes in traffic control commands can be detected automatically.

However, implementing such technologies requires skilled cybersecurity professionals and proper system integration.

5.5 Human Errors and Lack of Security Awareness

Human factors remain one of the important causes of cybersecurity failures. Even well-designed technical systems can become vulnerable because of incorrect configuration, weak passwords, improper access control, or lack of employee awareness.

Traffic control systems are managed by operators, administrators and technical staff. Errors such as failure to review alerts, incorrect log configuration, or delayed reporting of suspicious activities can reduce the effectiveness of security monitoring.

Regular cybersecurity training is necessary to improve awareness among employees. Staff should understand the importance of security logs, incident reporting procedures and safe handling of system information.

GYANBODH
An International Multidisciplinary Peer Reviewed Journal
ISSN:3048-9792
Volume: 3
Issue: 3
May - June: 2026

5.6 Insufficient Incident Response Mechanisms

Effective monitoring should be supported by a strong incident response process. Detecting a cyber threat without a proper response plan cannot prevent damage.

Many organizations face difficulties in:

- Identifying responsible teams during incidents.
- Preserving digital evidence.
- Communicating between technical departments.
- Recovering affected systems quickly.

For smart traffic infrastructure, incident response planning is especially important because disruption of services can directly affect public safety.

A well-defined incident response framework should include preparation, detection, containment, recovery and post-incident analysis. Regular security drills can help authorities evaluate their readiness.

5.7 Limited Compliance with Cybersecurity Standards

International cybersecurity standards provide structured approaches for protecting critical infrastructure. Frameworks such as the NIST Cybersecurity Framework, ISO/IEC 27001 and other security guidelines recommend proper logging, monitoring, risk assessment and incident management practices.

However, smart city projects often focus more on functionality and service delivery than cybersecurity maturity. Security measures may be added after system implementation rather than being included during the design stage.

For Ahmedabad Smart Traffic Control System, adopting standardized cybersecurity practices can improve security governance, accountability and operational reliability.

5.8 Privacy and Data Protection Challenges

Smart traffic systems collect large amounts of information through cameras, vehicle recognition systems and sensors. While this data supports traffic management, it also creates privacy concerns.

Security logs may contain sensitive information related to system users, vehicle identification records and operational activities. Poor access control or improper storage of such information may lead to unauthorized disclosure.

GYANBODH
An International Multidisciplinary Peer Reviewed Journal
ISSN:3048-9792
Volume: 3
Issue: 3
May - June: 2026

Therefore, monitoring systems should balance security requirements with privacy protection. Data encryption, restricted access and proper retention policies are necessary to protect collected information.

6. Recommendations

A centralized log management platform should be implemented to collect and analyse security logs from all components, including CCTV systems, IoT devices, servers, databases and network equipment.

A SIEM-based solution can provide:

- Centralized log collection.
- Automated event correlation.
- Real-time security alerts.
- Faster incident investigation.
- Better compliance management.

This approach will reduce information gaps and improve visibility across the entire traffic infrastructure.

Continuous monitoring should replace traditional periodic log reviews. Advanced analytics, artificial intelligence and machine learning techniques can help identify abnormal activities automatically.

AI-based monitoring systems can detect:

- Unusual login behaviour.
- Abnormal network traffic.
- Suspicious device activities.
- Possible malware infections.

Such technologies can improve early detection and reduce response time.

Since IoT devices are critical elements of smart traffic systems, their security should receive special attention. Recommended measures include:

- Strong device authentication.
- Encrypted communication.
- Secure firmware updates.
- Regular vulnerability testing.

GYANBODH
An International Multidisciplinary Peer Reviewed Journal
ISSN:3048-9792
Volume: 3
Issue: 3
May - June: 2026

- Standardized security logging.

Secure IoT management will reduce the possibility of attackers using connected devices as entry points.

7. Conclusion

Smart traffic systems have become essential components of modern urban management. Ahmedabad's adoption of intelligent traffic technologies has improved traffic monitoring, road safety and administrative efficiency. However, increasing dependence on connected technologies has introduced new cybersecurity challenges.

This study analysed security logging and monitoring failures in the Ahmedabad Smart Traffic Control System. The findings indicate that fragmented log management, insufficient real-time monitoring, IoT security limitations, human errors, weak incident response and limited cybersecurity standard adoption are major challenges.

Security logging and monitoring should be considered fundamental components of smart traffic infrastructure rather than optional security measures. Effective protection requires a combination of advanced technologies, skilled human resources, standardized processes and continuous improvement.

The implementation of centralized log management, AI-based monitoring, secure IoT practices, employee training, regular audits and international cybersecurity frameworks can significantly improve the reliability and security of Ahmedabad's smart traffic ecosystem.

As cities become increasingly dependent on digital infrastructure, cybersecurity will play a critical role in ensuring safe, efficient and trustworthy smart city services.

References

1. Amin, Manisha and Kirit Chokhawala (2026). IoT-Enabled Real-Time Decision Support System for Farm Automation. Research Genius. 11(21): 742-749.
2. Amin, Manisha and Kirit Chokhawala (2025). IOT-based field automation and monitoring in the Agriculture Sector. SURABHI: International Peer Reviewed Referred Journal. 100(2): 24-32.
3. Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. Computer Communications, 54, 1–31.

GYANBODH
An International Multidisciplinary Peer Reviewed Journal
ISSN:3048-9792
Volume: 3
Issue: 3
May - June: 2026

4. Cheng, L., Liu, F. and Yao, D. (2017). Enterprise data breach: Causes, challenges, prevention and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7(5), e1211.
5. European Union Agency for Cybersecurity. (2020). Cybersecurity challenges in the smart city environment. ENISA.
6. International Organization for Standardization. (2022). ISO/IEC 27001: Information security management systems—Requirements. ISO.
7. Khan, M. A. and Salah, K. (2018). IoT security: Review, blockchain solutions and open challenges. Future Generation Computer Systems, 82, 395–411.
8. National Institute of Standards and Technology. (2022). Cybersecurity framework. NIST.
9. National Institute of Standards and Technology. (2020). Guide to computer security log management (SP 800-92). NIST.
10. Pacheco, J. and Hariri, S. (2016). IoT security framework for smart cyber infrastructures. IEEE International Conference on Cloud Engineering, 246–251.
11. Patil, S. and Seshadri, R. (2021). Cybersecurity challenges in smart cities: A review. International Journal of Information Security Science, 10(2), 45–58.
12. Rathore, M. M., Ahmad, A., Paul, A. and Rho, S. (2016). Urban planning and building smart cities based on the Internet of Things using big data analytics. Computer Networks, 101, 63–80.
13. Stallings, W. (2020). Effective cybersecurity: A guide to using best practices and standards. Addison-Wesley.
14. Sicari, S., Rizzardi, A., Grieco, L. A. and Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164.
15. Singh, P. and Sharma, A. (2022). Security issues and challenges in smart city applications. Journal of Ambient Intelligence and Humanized Computing, 13, 3779–3793.
16. United Nations. (2021). Smart sustainable cities: A guide for policymakers. United Nations Publications.

GYANBODH
An International Multidisciplinary Peer Reviewed Journal
ISSN:3048-9792
Volume: 3
Issue: 3
May - June: 2026

17. Wang, S., Zhang, X., Zhang, Y. and Wang, L. (2021). Security and privacy issues in smart city applications. IEEE Access, 9, 123456–123470.
18. Zanella, A., Bui, N., Castellani, A., Vangelista, L. and Zorzi, M. (2014). Internet of Things for smart cities. IEEE Internet of Things Journal, 1(1), 22–32.