

Privacy-Preserving Smart City Traffic Management

Nihat Aksu

Baran Akkanat

Daan de Groot

1. Introduction

Traffic congestion has become a long-standing issue affecting densely populated urban areas, including the Netherlands. Daily congestion in Dutch cities has worsened due to rising population numbers, increasing car ownership rates, and expanding logistics operations. This process results in wasted resources and time, while also creating environmental harm through air pollution and increased CO₂ emissions. The rising number of vehicles on the road creates dangerous conditions for all road users, including drivers, cyclists, and pedestrians who must share crowded areas.

Artificial intelligence (AI) serves as the driving force behind smart city programs that municipalities implement to address these issues. Current systems function through real-time traffic observation and predictive modeling, which enable dynamic traffic light control adjustments. These advancements indicate that AI technology can effectively boost traffic management efficiency. However, such systems operate through the extensive collection of personal data, including video recordings, GPS tracking, and license plate identification. The use of personal data raises significant concerns about privacy protection, surveillance, and GDPR compliance.

This proposal seeks to establish a connection between operational traffic management and privacy protection. We introduce the concept of a privacy-preserving AI system for smart cities that enables municipalities to optimize traffic flows without violating the privacy rights of citizens. The project combines state-of-the-art AI techniques with responsible design principles to ensure that efficiency does not come at the cost of fundamental human rights.

Standard rule-based traffic management systems fail to adapt to modern urban environment changes because AI delivers critical assistance during this time. The system uses machine learning models to analyze information from multiple data streams which include video feeds and GPS signals and sensor readings for real-time operational optimization and fairness preservation. The implementation of AI through responsible design principles allows cities to build flexible traffic management systems which enhance traffic flow while maintaining data accessibility and privacy protection.

2. Problem Definition

The urban transportation system needs greater capacity to manage increasing traffic volumes while also reducing congestion and minimizing environmental pollution. Rising traffic congestion not only slows mobility but also increases the risk of accidents. Smart

systems can help address these challenges by identifying traffic patterns and pinpointing bottlenecks. Cameras installed along roads can support such solutions. When integrated with software, these cameras can detect and count vehicles. For instance, computer vision techniques such as edge detection [3] and image segmentation [1] have shown that software can effectively recognize vehicles.

However, current monitoring systems often rely on camera networks that do not always comply with GDPR regulations. For example, the municipality of Limerick (Ireland) was fined €110,000 for violating GDPR transparency requirements related to its smart CCTV pilot project [2]. As part of this project, 26 cameras were used for traffic management to help reduce congestion. According to Hersey [5], the system lacked a lawful basis for processing personal data collected by these cameras. In addition, live video feeds were shared with the national police of Ireland, which also constituted a breach of GDPR rules.

The key challenge is to enhance traffic flow management while safeguarding individual privacy. Without strong privacy protection measures, smart traffic management systems risk being perceived as tools of surveillance, which could lead to public resistance and ultimately compromise their effectiveness.

3. State of the Art

In recent years, research has increasingly focused on privacy-preserving methods for smart traffic management. It is essential that these approaches not only protect privacy but also perform competitively compared to existing systems. Moreover, such systems must be scalable to handle the vast amount of data collected from multiple sources. Cloud-based solutions can address scalability challenges, as they are capable of processing large volumes of data. However, they often suffer from latency issues due to the need to transmit data to and from the cloud.

To overcome these limitations, Rezaei et al.[7] proposes a scalable, low-latency, and privacy-preserving system called DST-FedRL. This system integrates federated edge AI, a Deep Spatial-Temporal Transformer Network (DST-Net), and reinforcement learning to detect vehicles in real time and optimize traffic routes. In DST-FedRL, data is processed locally on edge devices, such as traffic cameras, enabling scalable decision-making and minimizing latency. Federated Learning (FL) is employed to decentralize the training process and preserve data privacy. In federated learning, multiple agents collaboratively train a shared global model. In this study, each edge device trains a local DST-Net model using its locally collected data. After local training, devices send only the model updates (e.g., gradients or weight changes) to a central Federated Learning Coordinator, rather than transmitting raw data. This approach significantly enhances privacy and reduces data transmission overhead. The coordinator then aggregates the model updates to refine the global model. Once the global model is updated, it is redistributed to all edge devices, which continue training with newly collected local data, making the process iterative and continuously improving over time.

Traditional encryption algorithms are often computationally intensive, making them unsuitable for resource-constrained devices such as cameras. To address this issue, He et al. [4] propose a lightweight encryption algorithm designed specifically for use in such environments. This algorithm encrypts data in multiple layers, allowing users with different authorization levels to access images with varying degrees of detail. First, the algorithm encrypts the raw image data, which is then transmitted to a server. Unauthorized users only have access to the encrypted data. Users with Level 1 authorization can reconstruct

the image using a decryption algorithm, but sensitive elements such as license plates and windows remain automatically blurred. Users with Level 2 authorization can view images where only the license plate is visible, while Level 3 authorization grants access to fully reconstructed images showing both license plates and windows. This multilevel encryption approach effectively preserves privacy while still allowing authorized authorities to access the level of image detail necessary for their role. Figure 1 illustrates the different degrees of image anonymization that correspond to each level of authorization.

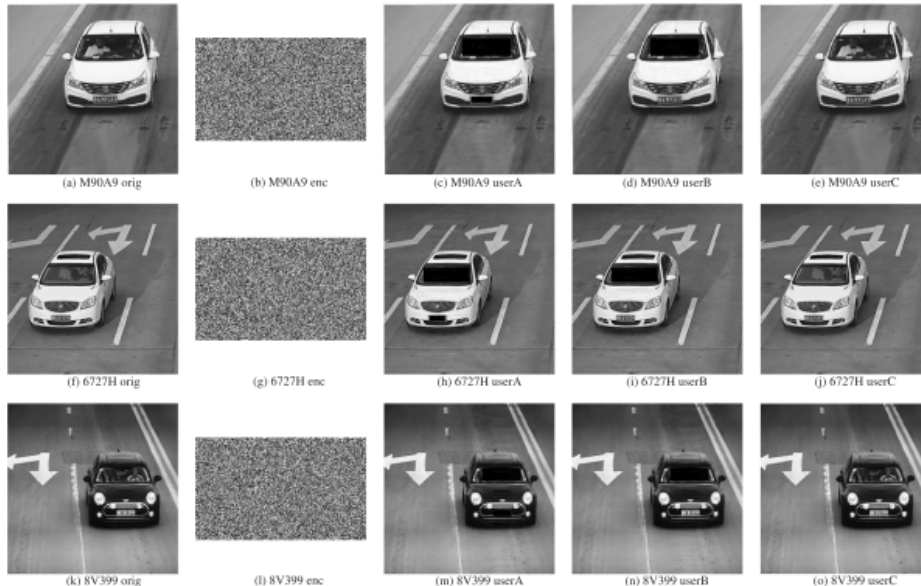


Figure 1: From left to right: original image, encrypted image, reconstructed image without privacy-related data, reconstructed image with the license plate visible, and reconstructed image with both the license plate and windows visible. [4]

In [6], the authors propose an algorithm that generates privacy-aware textual descriptions of raw image data. The algorithm, RL-MoE, combines Reinforcement Learning (RL) with a Mixture of Experts (MoE) model. The MoE model consists of multiple “experts,” each being a specialized neural network, a large language model (LLM), that focuses on a particular task. While MoE architectures are usually employed for general-purpose language understanding, this study adapts the approach so that each expert specializes in a specific privacy-relevant aspect of traffic images (e.g., vehicles, pedestrians, or road signs). Each expert receives the raw image as input and produces a privacy-aware textual description. In their implementation, four experts are used:

- Traffic Expert – Analyzes vehicle dynamics such as movement, congestion levels, and traffic flow using optical flow algorithms to estimate trajectories, vehicle density, and speed.
- Road Sign Expert – Detects and interprets road signs and other traffic control elements.
- Pedestrian Expert – Tracks pedestrians and performs pose estimation.
- Environment Expert – Extracts contextual information from the scene, such as weather conditions and visibility.

Each expert outputs a textual summary of its respective domain. These outputs are then aggregated to create a comprehensive description of the image. A reinforcement learning agent refines this combined text by selecting the most relevant information from each expert while maintaining conciseness and readability.

4. Proposed Solution

Local Context: Utrecht. The Municipality of Utrecht serves as a representative case study to demonstrate how the proposed method operates in privacy-protecting traffic management within the Netherlands. Utrecht, a rapidly expanding city of more than 360,000 residents, consistently ranks among Europe’s most bicycle-friendly municipalities. Three major intersections, Jaarbeursplein, Vredenburg, and the Central Station corridor, experience severe congestion during peak hours, where bicycles, cars, and public transport converge. The municipality operates several smart mobility initiatives, including adaptive traffic light control and mobility-as-a-service applications, which rely on real-time data streams containing personally identifiable information such as license plates and mobile device identifiers. The central challenge for Utrecht, as for many Dutch cities, lies in achieving traffic optimization while ensuring full compliance with the General Data Protection Regulation (GDPR) and maintaining public trust. The proposed system directly addresses these requirements by implementing edge computing for local anonymization and federated learning for distributed model training. Utrecht provides an ideal environment to evaluate responsible AI deployment because of its open-data policies and strong sustainability initiatives. The city’s goal of reducing CO₂ emissions by 40% by 2030 and its commitment to promoting cycling and public transport align with the ethical and environmental priorities of the proposed approach. Positioning the system within the Utrecht context therefore grounds the proposal in a realistic Dutch municipal framework, combining technical feasibility with genuine social, environmental, and regulatory relevance.

Real-life implementation: For our solution, we propose implementing a system based on [6] in a real-world environment specifically, in the city of Utrecht. We suggest conducting a pilot project in which the system provides early warnings to users about traffic congestion. This would enable the municipality to take proactive measures to reduce waiting times for residents and minimize the risk of accidents. The pilot would offer valuable insights into how well the system performs under real-world conditions, as it has so far only been tested on datasets. It would also provide researchers with practical feedback on the system’s efficiency and accuracy in delivering relevant information to the municipality. Furthermore, the pilot would allow an assessment of whether the system maintains the level of privacy preservation claimed in the original study, while still achieving high accuracy.

Dashboard Interface: Citizens could also access real-time textual descriptions of traffic congestion through a public dashboard. This would allow them to adjust their routes in case of severe congestion and provide greater insight into why the municipality has taken specific actions to address certain traffic situations.

5. Socio-Technical Embedding

Implementing an AI system in urban areas requires not only technical performance but also legal compliance, ethical safeguards, and public trust. Our solution integrates these requirements through socio-technical embedding.

Legal Compliance: The system is designed in accordance with the General Data Protection Regulation (GDPR). Data minimization ensures that only necessary, non-identifiable information is processed. Privacy-by-design and privacy-by-default principles are incorporated at the architectural level.

Citizen Trust and Transparency: Citizens must trust and understand the system. The dashboard provides clear explanations of which privacy features are active and demonstrates that no personal surveillance takes place.

Human Oversight: Human traffic operators remain in the loop to avoid full automation. AI recommendations can be overridden in emergencies, accidents, or system malfunctions.

Ethical Safeguards: Equal service delivery across all geographic areas prevents discrimination. System performance monitoring across neighborhoods enables the detection of algorithmic bias and allows developers to adjust models accordingly.

Societal Impact: Improved traffic flow reduces CO2 emissions and creates safer conditions for cyclists and pedestrians. This supports national sustainability goals while fostering public trust in AI-based governance.

By embedding technological features within legal, ethical, and social frameworks, the system demonstrates responsible AI practices and builds credibility as an innovative approach.

The method follows the Socio-Technical Systems Theory which studies how technology and human actors and institutional structures develop together. The framework depends on AI development to maintain technological progress in alignment with social values through established governance principles. The project implements Responsible AI principles through transparency and human oversight and accountability systems to ensure public interest alignment with automation.

6. Design Process

The system development process follows an iterative approach that incorporates stakeholder participation to fulfill both technical and social requirements. The process includes:

Problem Analysis: Review existing traffic data to identify congestion hotspots and assess GDPR requirements.

Stakeholder Engagement: Consult municipalities, traffic authorities, citizens, regulators, and environmental organizations to gather requirements. Surveys and workshops capture diverse perspectives.

System Architecture Design: Define technical components (edge computing units, federated learning nodes, privacy layers) and create a conceptual dashboard mock-up.

Mock-Up Development: Produce prototype visuals of the system interface showing both successful traffic optimization (happy flow) and system failures (sad flow).

Evaluation and Feedback: Present mock-ups to stakeholders for feedback on usability, transparency, and trustworthiness, then refine the design accordingly.

Iterative Refinement: Continuously improve the system by cycling through design, testing, and evaluation until both technical and socio-ethical standards are satisfied.

This structured process ensures operational reliability by meeting technical specifications and achieving social acceptance, transparency, and adaptability.

7. Stakeholders

The operation of a privacy-preserving traffic management system requires collaboration among multiple stakeholders.

Municipal Governments and Traffic Authorities: These institutions serve as the main operators and decision-makers. They deploy the system, interpret outputs, and make policy decisions such as traffic light adjustments and rerouting. Their main concerns are efficiency, safety, and public trust.

Citizens (Drivers, Cyclists, Pedestrians): Citizens are the end beneficiaries. They expect smoother travel, reduced delays, and safer roads without intrusive surveillance. Their concerns focus on data privacy and equal service quality across neighborhoods.

Technology Providers: AI developers, hardware manufacturers, and infrastructure companies build and maintain the system. Their priorities include technical feasibility, reliability, and securing long-term contracts with municipalities.

Regulators and Policymakers: These actors ensure compliance with GDPR and ethical standards. They monitor accountability and verify that the system operates within legal boundaries.

Environmental Organizations: As secondary stakeholders, they monitor the system’s contribution to reducing emissions and promoting sustainability. They may also advocate for public support.

Clear identification of stakeholders and their roles allows the system design to address diverse needs and achieve widespread acceptance.

Stakeholder	Needs/Interests	Concerns
Municipalities	Efficient traffic flow	Cost of GDPR compliance
Citizens	Safer, faster mobility	Loss of privacy / surveillance
Tech Providers	Long-term contracts	Technical feasibility
Regulators	Accountability, GDPR	Transparency of decisions
Environmental NGOs	Reduced CO ₂ emissions	Impact measurability

Table 1: Stakeholder Needs and Concerns

8. Happy and sad flow

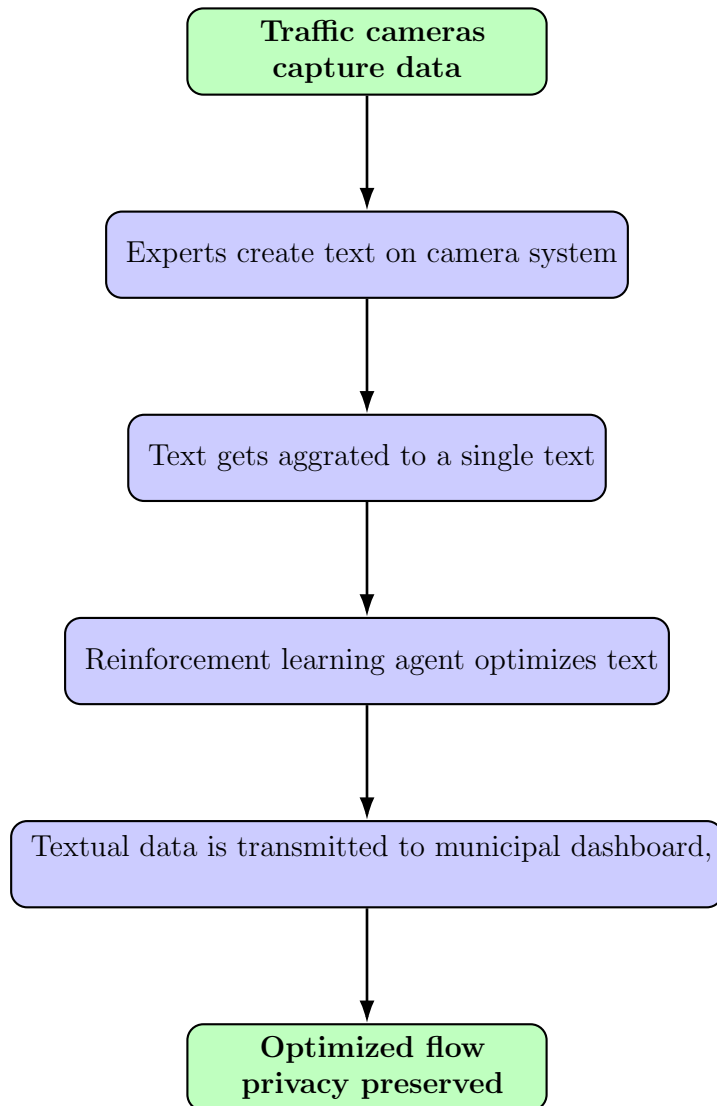


Figure 2: Happy flow of the proposed system

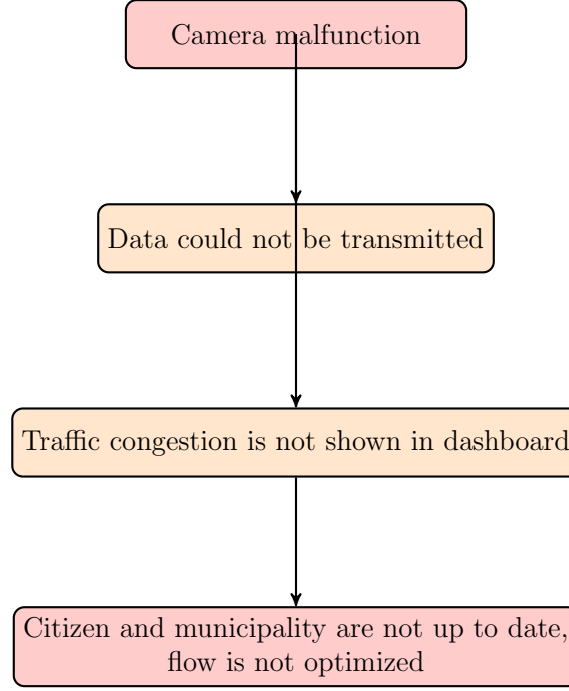


Figure 3: Sad flow of the proposed system

9. Justification for the use of AI

In this paper, we propose the use of an AI model to translate images into privacy-preserving textual descriptions. By applying this approach, the privacy of citizens is significantly enhanced, as no raw image data is transmitted to a central server. This ensures that sensitive information, such as license plates or faces, cannot be viewed by unauthorized individuals. Given that camera-based systems without privacy-preserving mechanisms have been shown to risk privacy breaches, as demonstrated in [2], the implementation of this system is well justified.

10. Novelty

AI-based traffic management systems exist, but most rely on centralized data collection without prioritizing privacy. Our proposed system is a privacy-preserving innovation:

- By using an AI model to translate visual data into textual descriptions, citizens' privacy can be significantly better protected, as no sensitive information, such as license plates or faces, is transmitted to a central server.
- By providing citizens with access to a public dashboard, they gain better insight into why the municipality takes specific actions to manage traffic congestion. This increased transparency can help citizens understand decision-making processes more clearly and strengthen their trust in local government.
- By testing the system in a real-life scenario, we can gain new insights into its practical performance. Key questions include whether the system is sufficiently scalable, whether privacy is preserved to the extent claimed in theory, and whether it can effectively handle new, real-world data.

The novelty lies not in inventing new algorithms but in responsibly adapting advanced AI methods to a critical domain where privacy and trust are essential.

11. Limitations and Future Work

Although the proposed privacy-preserving traffic management architecture demonstrates technical feasibility, several implementation challenges remain. Deploying such a system at scale in urban environments may require substantial computational resources and financial investment. Each intersection would need suitable hardware and stable network connectivity to enable on-device processing. At present, the system has only been evaluated conceptually and through design mock-ups rather than real-world deployment. Future research should involve collaboration with Utrecht’s municipal traffic authority to pilot the system using live intersection data. Such a deployment would allow empirical evaluation of key performance indicators such as latency, prediction accuracy, and privacy leakage risk. In parallel, user studies should investigate how citizens perceive transparency dashboards and whether these features genuinely enhance public trust in AI-based governance. Finally, policy-oriented work is needed to establish guidelines for privacy-preserving AI implementation across Dutch municipalities, ensuring consistent standards for responsible smart city governance.

12. Conclusion

Traffic congestion poses both practical and societal challenges for modern cities. While AI offers significant potential to optimize urban mobility, its reliance on personal data raises concerns about privacy and public trust. Our proposed system demonstrates that operational efficiency and privacy protection can coexist. By integrating our model, municipalities can ensure GDPR compliance while maintaining effective traffic management.

Transparency features and human oversight further strengthen public trust and support the responsible deployment of AI technologies. Testing the system in a real-world setting provides researchers with valuable insights into its performance beyond theoretical conditions. Ultimately, this project contributes to broader societal goals by reducing emissions, improving safety, and promoting sustainability. It offers municipalities a concrete framework for ethical AI adoption and serves as a model for future smart city innovations.

Feature	Current Systems	Proposed System
Data Collection	Centralized, raw video/GPS storage	Local processing at edge devices with anonymization
Privacy	Weak: faces and license plates often stored	Strong: no raw data, only textual privacy-preserving description
Compliance	GDPR violations likely due to raw data retention	GDPR compliance by design (privacy-by-default and minimization)
Transparency	Limited explanations of how data is processed	Dashboard shows traffic congestion's and why actions are taken by municipality

Table 2: Comparison of Current Traffic Systems and the Proposed Privacy-Preserving System

References

- [1] Ake, A.A.R., Pereira, B., Bakhshi, R., Govani, A.: Tracking and segmentation of vehicles in traffic video (02 2024). <https://doi.org/10.13140/RG.2.2.25186.30407>
- [2] Dixon, H.: In the matter of the general data protection regulation and the data protection act 2018: Dpc case reference 03/siu/2018 (12 2021), https://www.dataprotection.ie/sites/default/files/uploads/2022-01/REDACTED_091221_Final%20DecisionLimerick_03-SIU-2018%20PDF%20FINAL.pdf, accessed: 2025-10-05
- [3] Dwivedi, A.D., Singh, A.K., Kumar, P.: Smart traffic management system. International Journal for Research in Applied Science and Engineering Technology (IJRASET) (05 2023). <https://doi.org/10.22214/ijraset.2023.53186>, <https://www.ijraset.com/research-paper/smart-traffic-management-system>
- [4] He, X., Haipeng, P., Tong, F.: Multi-level privacy-preserving scheme for image extraction based on compressive sensing in intelligent traffic management. Signal Processing **220**, 109445 (03 2024). <https://doi.org/10.1016/j.sigpro.2024.109445>
- [5] Hersey, F.: Irish municipality fined for gdpr non-compliant cameras, finland devises centralized system. Biometric Update (02 2022), <https://www.biometricupdate.com/202202/irish-municipality-fined-for-gdpr-non-compliant-cameras-finland-devises-centralized>, accessed: 2025-10-05
- [6] Mohankumar, C., Arunachalam, M.: Decentralized traffic management with federated edge ai: a reinforced transnet model for real-time vehicle object detection and collaborative route optimization. Discover Applied Sciences **7** (07 2025). <https://doi.org/10.1007/s42452-025-07383-6>
- [7] Rezaei, A., Sookhak, M., Haghparast, M.: Rl-moe: An image-based privacy preserving approach in intelligent transportation system (08 2025). <https://doi.org/10.48550/arXiv.2508.09186>