



Paper Type: Original Article

## Designing Secure-by-Design IoT for Smart Transportation: A Privacy-Aware Data Analytics

Sanaz Hami Hassan Kiyadeh<sup>1,\*</sup> , Hamiden Abd El-Wahed Khalifa<sup>2</sup> 

<sup>1</sup> Department of Mathematics, The University of Alabama, Tuscaloosa, 35487 Alabama, USA; shkiyadeh@crimson.ua.edu.

<sup>2</sup> Operations Research Department, Faculty of Graduate Studies for Statistical Research, Cairo University, 12613 Giza, Egypt; hamiden@cu.edu.eg.

### Citation:

Received: 11 March 2025

Revised: 12 May 2025

Accepted: 28 June 2025

Hami Hassan Kiyadeh, S., & Abd El-Wahed Khalifa, H. (2025). Designing secure-by-design IoT for smart transportation: A privacy-aware data analytics. *Smart City Insights*, 2(3), 125-135.


### Abstract


Many cities have adopted smart city initiatives recently and have seen significant improvements in the services they offer to society and the environment. They are equipped to manipulate real-time physical entities and to disseminate smart information to people through smart transportation, healthcare, smart buildings, smart public security, smart parking, intelligent traffic systems, and agriculture. Someone can extract sensitive information from smart city applications. However, user resistance is the most common concern regarding privacy and security. Therefore, while designing and developing the applications, it is also pertinent to understand these security and privacy issues. This paper centers on the critical areas of smart city application and identifies concerns related to an integrative architecture of privacy and security by design. It also evaluates some of the existing approaches to the problems of security and privacy in information technology, which are core to the effective performance of smart city applications. It outlines areas for further research that still require attention to enhance performance.

**Keywords:** Smart transportation, Intelligent traffic systems, Smart public security, Integrative architecture, Real-time data.

## 1 | Introduction

The interconnectedness of systems leveraging IoT technology and the concept of intelligent transportation systems is realized, as it eases the supervision and alteration of traffic conditions [1]. The advancement of civilization directly reduces emissions and the abundance of engines [2]. Traffic congestion will be eased, enhancing vehicle and pedestrian safety and making the transport system more efficient and better controlled overall. Users' privacy in these systems is somewhat concerning, as the ITS collects information on public transport systems and user travel patterns [3]. Many primary requests concern the large amounts of data and

 Corresponding Author: shkiyadeh@crimson.ua.edu

 <https://doi.org/10.22105/sci.v2i3.41>



Licensee System Analytics. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

information requisitioned by ITS related to vehicles, their positions, and drivers' profiles, emphasizing information that goes well beyond the onboard [4]. However, these breaches of privacy occur when the information collected is used inappropriately, i.e., erroneously. In this case, the lack of privacy and security for certain data is the most fundamental challenge in the context of ITS [5]. Different kinds of system attacks can be aimed at and inflicted against ITS. Such attacks affect the system and cause customer emergency response systems to malfunction for extended periods. To identify potential privacy risks and provide recommendations on the use of IT in ITS, conduct a PIA. Hence, this paper must examine the dilemmas and risks associated with elegant transportation systems [6].

## 2 | Background and Related Work

### 2.1 | IoT Technologies in Transportation

IoT applications in transportation involve an interconnected network of devices and systems, such as sensors, actuators, analytics platforms, and cloud-based solutions [7]. Core components include:

**Sensors and GPS:** these devices collect data on vehicle location, traffic patterns, and environmental factors [4].

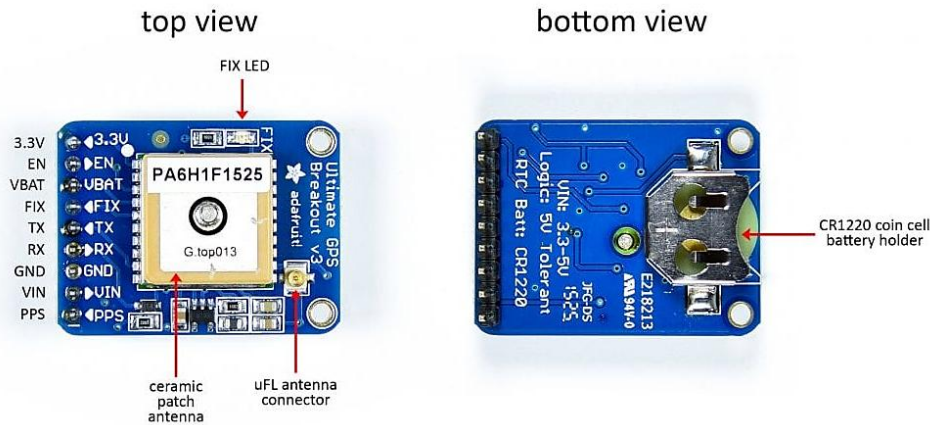


Fig. 1. Top and bottom views of the GPS module used in intelligent transportation systems.

**RFID and cameras:** RFID tags help track vehicles, while cameras monitor congestion, supporting effective traffic management and automated tolling [8].

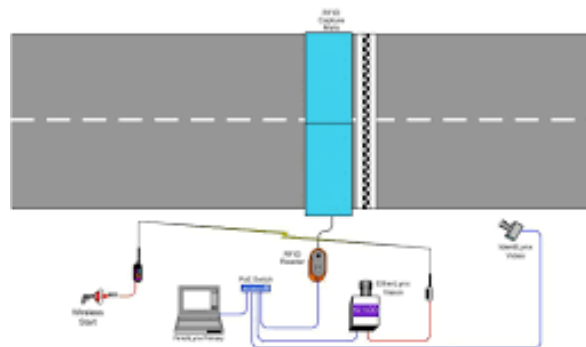


Fig. 2. RFID- and camera-based vehicle monitoring system.

**Communication protocols:** technologies such as 5G, Wi-Fi, Zigbee, and Dedicated Short-Range Communication (DSRC) enable real-time data exchange between devices and central systems, ensuring high-speed, low-latency communication, which is essential to IoT [9].

Together, these components create a framework for smart traffic management, vehicle tracking, and improved passenger safety, forming the foundation of intelligent transportation networks [10].

## 2.2 | Evolution of Security and Privacy in IoT

As IoT increasingly integrates into critical infrastructure, such as transportation, specific security and privacy practices have been developed to address unique challenges [11]. Initial research concentrated on device security and encryption for communication and data management [12]. As IoT systems expanded, the focus shifted to network security, intrusion detection, and privacy measures to address new threats and safeguard user data from unauthorized access [13].

## 2.3 | Related Work on Security and Privacy in IoT-Enabled Transportation

Several studies have examined security issues in IoT-powered transportation networks. For example, Wu et al. [14] analyzed intrusion detection methods for vehicular networks, while Zhang et al. [15] researched privacy-preserving techniques for data aggregation. Emerging work on blockchain applications within IoT highlights the potential of decentralized security for transportation systems [16]. However, further research is needed to address challenges such as high mobility and dynamic network connectivity, especially for real-time security responses [17].

## 2.4 | Identified Gaps and Research Objectives

Despite progress in IoT security, there are still areas that need attention, such as managing real-time threats and designing systems capable of meeting high-speed, low-latency demands. Moreover, balancing user privacy with data usability for operational purposes remains underexplored [6]. This paper addresses these gaps by evaluating existing approaches and proposing new directions to enhance security and privacy in smart transportation systems [17].

## 3 | Security Threats in IoT-Enabled Smart Transportation

IoT-enabled smart transportation systems encounter a wide range of security threats that can compromise network integrity, device reliability, and data confidentiality [11]. These threats can be categorized into three main types: network-level threats, device-level threats, and data-related threats [18].

### 3.1 | Network-Level Threats

Network-level threats target the communication infrastructure of IoT-based transportation systems. Key examples include:

**Distributed Denial of Service (DDoS) attacks:** DDoS attacks overwhelm networks, hindering legitimate service access. In a transportation context, such attacks can disrupt traffic signal operations or Vehicle-to-Vehicle (V2V) communication, resulting in congestion and an increased likelihood of accidents [19].

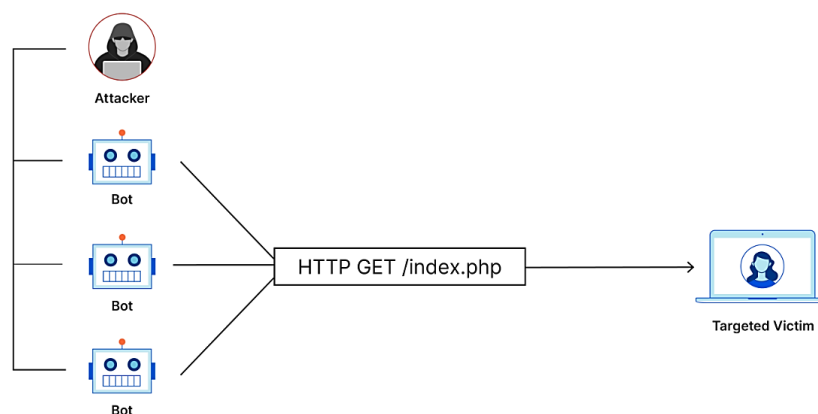
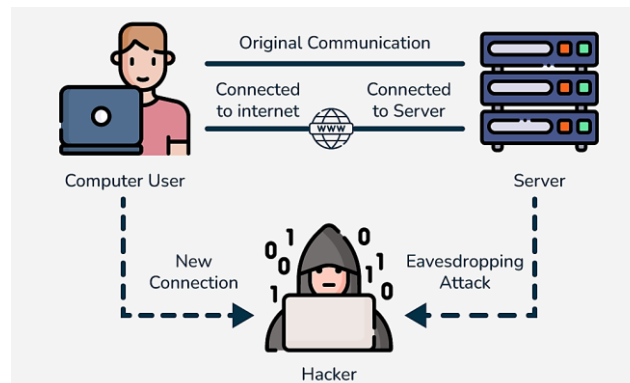


Fig. 3. Distributed Denial of Service (DDoS) attack model in IoT-based.

Eavesdropping and spoofing: attackers may intercept or manipulate communications between devices, impersonating legitimate users or injecting false information to disrupt transportation operations [20].



**Fig. 4. Network-level interception and impersonation attack in smart transportation systems.**

Unauthorized access: insufficient access controls can allow unauthorized individuals to access network resources, potentially leading to the misuse of sensitive information or operational disruptions [21].

### 3.2 | Device-Level Threats

Device-level threats target vulnerabilities inherent to individual IoT devices in transportation networks. Common issues include:

**Weak authentication:** Many IoT devices operate with default or inadequate passwords, making them easy targets for unauthorized access.

**Firmware vulnerabilities:** devices with unpatched firmware are exposed to malware, which may compromise functionality or allow attackers to access sensitive information.

**Physical tampering:** when IoT devices are physically accessible, as in public transportation or roadside installations, they are compromised, underscoring the need for robust security measures.

### 3.3 | Data-Related Threats

Data-related threats jeopardize the confidentiality, integrity, and availability of information within IoT-enabled transportation systems:

**Data manipulation:** tampered data can lead to incorrect traffic management and route optimization decisions [22].

**Data breaches:** unauthorized access to personal data, such as user travel patterns, can violate privacy and expose individuals to risks, including stalking [23].

**Data loss:** hardware failures or cyberattacks can result in data loss, negatively affecting transportation operations and the reliability of predictive analytics [24].

### 3.4 | Case Studies of Security Breaches

Recent incidents illustrate the real-world consequences of security breaches in IoT-enabled transportation. For instance, in 2017, a hacker accessed traffic light control systems in Dallas, Texas, resulting in significant congestion and operational delays. Additionally, vulnerabilities in the wireless communication protocols of autonomous vehicles have been exploited, allowing attackers to interfere with vehicle control systems. These cases highlight the urgent need for enhanced security measures to safeguard transportation infrastructure against malicious threats.

## 4 | Privacy Concerns in IoT-Enabled Smart Transportation

Integrating IoT technology into smart transportation systems poses significant privacy challenges, particularly regarding the collection and management of personal data. Concerns arise from the ability to track users' locations, behaviors, and preferences, often without explicit consent or effective data protection measures in place [3].

### 4.1 | Location and Movement Tracking

IoT systems in transportation continually track vehicle locations and travel paths, offering comprehensive insights into individual movements. If this information is improperly accessed or exploited, it could violate user privacy by exposing sensitive details about personal habits and locations. The issue of location tracking is particularly contentious in public transport, where users may be unaware of or not consent to data collection.

### 4.2 | Personal Data Collection and Usage

In addition to tracking locations, IoT systems gather information on user preferences, travel history, and payment information. While this data collection can enhance service efficiency, it also poses risks, such as identity theft and targeted surveillance, if not adequately protected. Furthermore, data originally collected for operational reasons might be reused for commercial purposes without users' explicit consent, thereby infringing on essential data privacy rights.

### 4.3 | Risks of Data Aggregation and Re-identification

Data that is not properly anonymized can often be traced back to specific individuals through re-identification methods. When IoT transportation systems aggregate data for analytical purposes, safeguarding user privacy becomes increasingly difficult. Studies have shown that aggregated data, when analyzed alongside other datasets, can lead to privacy breaches even when personal identifiers have been removed [25].

### 4.4 | Legal and Ethical Implications

Privacy regulations, such as the EU's General Data Protection Regulation (GDPR), are designed to protect individual data by requiring transparency, user consent, and data protection. However, the international nature of transportation networks makes compliance challenging due to differing privacy laws across regions. Additionally, ethical considerations arise, as transportation operators must protect personal information while striving for operational efficiency and service enhancements.

### 4.5 | Instances of Privacy Breaches

There have been numerous incidents of privacy breaches within IoT-enabled transportation systems worldwide. Examples include unauthorized surveillance in London's public transport systems and the mishandling of passenger data by third-party companies across various ride-sharing services. Such breaches undermine user trust and expose transportation agencies to legal liability, underscoring the urgent need for effective privacy protection strategies.

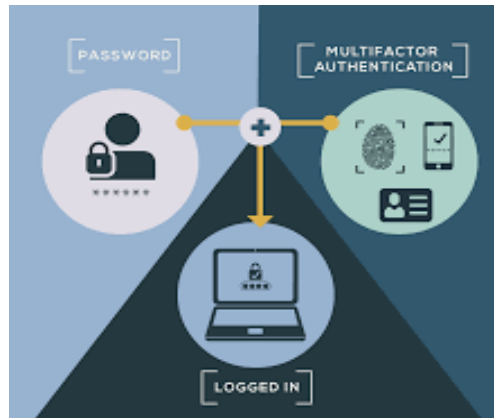
## 5 | Technical Solutions for Security and Privacy

A variety of technical strategies have proposed and implemented to address the security threats and privacy challenges in IoT-enabled smart transportation networks. These strategies focus on strengthening system resilience against attacks while protecting user information.

### 5.1 | Authentication and Access Control

Robust authentication and access control measures are crucial for protecting IoT devices and networks.

**Multi-Factor Authentication (MFA):** MFA enhances security by requiring users to provide two or more verification forms before granting access. For example, transportation authorities could adopt MFA for system administrators managing traffic control systems, utilizing a combination of passwords, security tokens, and biometric identification. It significantly lowers the chances of unauthorized access [26].



**Fig. 6. Authentication and access control using multi-factor verification.**

**Role-Based Access Control (RBAC):** Implementing RBAC allows organizations to assign permissions based on user roles within the system. For instance, only designated personnel should be allowed to adjust traffic signal settings or access sensitive user information. This approach reduces exposure and safeguards critical infrastructure from insider threats [27].

#### Role-based access control



**Fig. 6. Authentication and access control mechanisms in IoT-enabled smart transportation systems.**

## 5.2 | Encryption Techniques

Encryption is essential for securing data during transmission and at rest within IoT networks.

**End-to-End Encryption (E2EE):** E2EE ensures that data exchanged between IoT devices and central servers remains encrypted throughout transmission. It means that even if an attacker intercepts the data, they cannot decrypt it without the appropriate keys. For example, vehicle-to-vehicle (V2V) communications can use end-to-end (E2EE) encryption to protect against eavesdropping.

**Public Key Infrastructure (PKI):** PKI enables secure device-to-device communication through asymmetric encryption. In the transportation sector, PKI can verify devices before they interact, ensuring only trusted devices are connected to the network.

### 5.3 | Intrusion Detection and Prevention Systems

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) monitor network traffic and device activity to identify and respond to potential threats.

Network-based and host-based IDS: A network-based IDS monitors traffic across the network, while a host-based IDS evaluates activities on individual devices. Both systems can identify anomalies that may indicate security breaches. For instance, an IDS might detect unusual traffic patterns from a specific vehicle, suggesting a possible compromise [28].

Machine learning in intrusion detection: leveraging machine learning algorithms in IDS enhances the system's ability to learn from historical data and more effectively identify emerging threats. By continuously adapting to new normal behavior patterns, these systems can provide timely alerts for potential security incidents.

### 5.4 | Blockchain for Decentralized Security

Blockchain technology is innovative in enhancing security and privacy in IoT-enabled transportation networks.

Immutable ledger for transaction security: blockchain creates an unchangeable record of all transactions, particularly useful for documenting vehicle interactions and traffic data. This transparency ensures that data cannot be altered retroactively, providing an audit trail that increases accountability [29].

Smart contracts for automated security protocols: Smart contracts enable automated enforcement of predefined security measures when specific conditions are met. For example, a smart contract could automatically revoke access to a vehicle's control system if a potential security breach is detected [30].

## 6 | Privacy-Preserving Data Processing

As IoT systems generate extensive amounts of data, it is crucial to protect user privacy while leveraging this data to improve operational efficiency. Several advanced methodologies have been developed to strike this balance.

### 6.1 | Federated Learning

Federated learning is a decentralized approach to machine learning that enables devices to collaboratively develop a shared model while keeping their data local.

Data locality and privacy: rather than transmitting raw data to a central server, devices train a model locally and only share model updates. This method significantly reduces the risk of data exposure, as sensitive information remains on the device. For example, public transportation systems can analyze passenger usage patterns without disclosing individual identities [31].

### 6.2 | Differential Privacy

Differential privacy introduces noise into datasets to protect individual entries while permitting meaningful data analysis.

Safeguarding user identity: differential privacy ensures that the results of data analyses do not disclose sensitive information about any particular user by adding randomness to datasets. For instance, traffic data can be aggregated to remain valuable for operational decisions without compromising individual drivers' privacy [32].

### 6.3 | Secure Multiparty Computation

Secure Multiparty Computation (SMPC) allows multiple parties to compute functions based on their inputs while keeping those inputs confidential.



Collaborative data analysis: in the transportation sector, stakeholders (such as public transport agencies and vehicle manufacturers) can analyze data together to generate shared insights without exposing sensitive information. For example, a city might study traffic patterns using data from different ride-sharing services without needing access to proprietary user data from those companies [33].

## **7 | Challenges and Limitations**

Although various strategies are available to bolster security and privacy in IoT-enabled smart transportation systems, several challenges and limitations persist.

### **7.1 | Technical Limitations**

Many IoT devices have restricted processing power and storage capabilities, which can impede the deployment of sophisticated security measures. These devices are often designed to focus on efficiency and cost-effectiveness, making it difficult to implement strong encryption or advanced security protocols [34].

### **7.2 | Financial Limitations**

The expenses for implementing advanced security solutions can be substantial, especially for smaller municipalities or organizations with constrained budgets. Financial investments in security measures often compete with other operational costs, leading to insufficient funding for essential security initiatives.

### **7.3 | Regulatory Challenges and Interoperability**

The absence of standardized security protocols across various IoT devices and platforms complicates the development of unified security frameworks. Moreover, the international nature of transportation networks means that adhering to differing regional regulations can be cumbersome, making it challenging for organizations to ensure comprehensive data protection.

## **8 | Future Directions and Research Opportunities**

Several future research avenues should be explored to effectively tackle the changing security and privacy challenges in IoT-enabled smart transportation.

### **8.1 | Enhancing IoT Device Security**

Future research should focus on developing IoT devices with built-in security features, such as Hardware Security Modules (HSMs) that provide secure key management and storage. This approach would significantly bolster the network's overall security.

### **8.2 | Utilizing Artificial Intelligence for Threat Detection**

Progress in Artificial Intelligence (AI) and machine learning has the potential to greatly improve threat detection capabilities. Future studies could investigate the development of AI-based models that continuously learn from emerging threats and adapt their responses in real-time [28].

### **8.3 | Fostering Public-Private Partnerships for Enhanced Security**

Collaboration among public agencies, private-sector companies, and academic institutions can enable the sharing of threat intelligence, resources, and best practices, thereby strengthening security standards across the transportation industry.



## 8.4 | Investigating Quantum-Resistant Security Algorithms

As quantum computing advances, conventional encryption methods may become vulnerable. Therefore, researching quantum-resistant cryptographic algorithms is essential to ensure the long-term security of IoT-enabled systems.

## 9 | Conclusion

Incorporating IoT technologies within transportation networks offers significant potential for improved efficiency and safety. However, the security and privacy issues that arise require a thorough strategy to safeguard users and systems. By adopting strong security practices, leveraging advanced privacy-preserving methods, and fostering cross-sector cooperation, we can establish a secure and reliable framework for IoT-enabled smart transportation systems. Ongoing research should focus on identifying new threats and creating adaptive solutions to address the challenges posed by this evolving environment.

## Acknowledgments

I want to express my sincere appreciation to all those who assisted me in researching and writing this paper.

First and foremost, I am deeply thankful to my academic advisors and mentors for their invaluable support and encouragement. Their knowledge and insights were crucial in enhancing my understanding of the intricate issues related to security and privacy in IoT-enabled smart transportation networks. I also want to recognize the constructive feedback from my peers and colleagues. Their engaging discussions and critical viewpoints significantly enriched the quality of my research. I am particularly grateful to the institutions and scholars whose work I cited in this paper. Their commitment to expanding knowledge in IoT, cybersecurity, and transportation systems has profoundly influenced my research.

Finally, I acknowledge the steadfast support of my family and friends. Their encouragement and patience were essential as I faced the various challenges of this research. I hope this paper adds value to ongoing discussions in this vital field and encourages future advancements in secure, efficient transportation systems.

## Data Availability

I advocate for transparency in research by promoting public access to data. However, this study did not generate any new data. The results presented in this paper are derived from a thorough review of existing literature and publicly accessible datasets about IoT-enabled smart transportation networks.

The datasets examined in this research can be located in the following publicly available archives:

UCI machine learning repository: This repository offers a variety of datasets relevant to smart transportation systems, suitable for further investigation.

Kaggle datasets: Kaggle features numerous datasets related to transportation, IoT, and security, which can yield valuable insights for future research.

Transportation Research Board (TRB) publications: TRB provides access to many publications and datasets focused on transportation research.

It is important to note that specific datasets that include sensitive user information have not been disclosed due to privacy and ethical considerations. The data utilized in this paper adhere to all relevant ethical standards and data protection regulations.

## Conflicts of Interest

The author declares no conflict of interest. I affirm that no personal circumstances or interests could be perceived as having an inappropriate influence on the presentation or interpretation of the research findings.

reported in this paper. Furthermore, funders played no role in the design of the study, the collection, analysis, or interpretation of the data, the writing of the manuscript, or the decision to publish the results.

## References

- [1] Elassy, M., Al-Hattab, M., Takruri, M., & Badawi, S. (2024). Intelligent transportation systems for sustainable smart cities. *Transportation engineering*, 16, 100252. <https://doi.org/10.1016/j.treng.2024.100252>
- [2] Lv, Z., & Shang, W. (2023). Impacts of intelligent transportation systems on energy conservation and emission reduction of transport systems: A comprehensive review. *Green technologies and sustainability*, 1(1), 100002. <https://doi.org/10.1016/j.grets.2022.100002>
- [3] Islami, L., Fischer-Hübner, S., & Papadimitratos, P. (2022). Capturing drivers' privacy preferences for intelligent transportation systems: An intercultural perspective. *Computers & security*, 123, 102913. <https://doi.org/10.1016/j.cose.2022.102913>
- [4] Micko, K., Papcun, P., & Zolotova, I. (2023). Review of IoT sensor systems used for monitoring the road infrastructure. *Sensors*, 23(9), 4469. <https://doi.org/10.3390/s23094469>
- [5] Vu, L., Suo, K., Islam, M. R., Dhar, N., Nguyen, T. N., He, S., & Shi, Y. (2024). *Living on the electric vehicle and cloud era: A study of cyber vulnerabilities, potential impacts, and possible strategies* [presentation]. Proceedings of the 2024 acm southeast conference (pp. 18–26). <https://doi.org/10.1145/3603287.3651209>
- [6] Aslam, M. M., Shafik, W., Hidayatullah, A. F., Kalinaki, K., Gul, H., Zakari, R. Y., & Tufail, A. (2025). Intelligent transportation systems: A critical review of integration of cyber-physical systems (CPS) and Industry 4.0. *Digital communications and networks*. <https://doi.org/10.1016/j.dcan.2025.06.014>
- [7] Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: A survey. *Future generation computer systems*, 56, 684–700. <https://doi.org/10.1016/j.future.2015.09.021>
- [8] Khazukov, K., Shepelev, V., Karpeta, T., Shabiev, S., Slobodin, I., Charbadze, I., & Alferova, I. (2020). Real-time monitoring of traffic parameters. *Journal of big data*, 7(1), 84. <https://doi.org/10.1186/s40537-020-00358-x>
- [9] Rammohan, A. (2023). Revolutionizing intelligent transportation systems with cellular vehicle-to-everything (C-V2X) technology: Current trends, use cases, emerging technologies, standardization bodies, industry analytics and future directions. *Vehicular communications*, 43, 100638. <https://doi.org/10.1016/j.vehcom.2023.100638>
- [10] Mendes, B., Araujo, M., Goes, A., Corujo, D., & Oliveira, A. S. R. (2025). Exploring V2X in 5G networks: A comprehensive survey of location-based services in hybrid scenarios. *Vehicular communications*, 100878. <https://doi.org/10.1016/j.vehcom.2025.100878>
- [11] Sebestyen, H., Popescu, D. E., & Zmaranda, R. D. (2025). A literature review on security in the internet of things: Identifying and analysing critical categories. *Computers*, 14(2), 61. <https://doi.org/10.3390/computers14020061>
- [12] Malhotra, P., Singh, Y., Anand, P., Bangotra, D. K., Singh, P. K., & Hong, W. C. (2021). Internet of things: Evolution, concerns and security challenges. *Sensors*, 21(5), 1809. <https://doi.org/10.3390/s21051809>
- [13] Sun, P., Wan, Y., Wu, Z., Fang, Z., & Li, Q. (2025). A survey on privacy and security issues in IoT-based environments: Technologies, protection measures and future directions. *Computers & security*, 148, 104097. <https://doi.org/10.1016/j.cose.2024.104097>
- [14] Wu, W., Li, R., Xie, G., An, J., Bai, Y., Zhou, J., & Li, K. (2019). A survey of intrusion detection for in-vehicle networks. *IEEE transactions on intelligent transportation systems*, 21(3), 919–933. <https://doi.org/10.1109/TITS.2019.2908074>
- [15] Zhang, M., Yang, L., He, S., Li, M., & Zhang, J. (2021). Privacy-preserving data aggregation for mobile crowdsensing with externality: An auction approach. *IEEE/ACM transactions on networking*, 29(3), 1046–1059. <https://doi.org/10.1109/TNET.2021.3056490>
- [16] Obaidat, M. A., Rawashdeh, M., Alja'afreh, M., Abouali, M., Thakur, K., & Karime, A. (2024). Exploring IoT and blockchain: A comprehensive survey on security, integration strategies, applications and future research directions. *Big data and cognitive computing*, 8(12), 174. <https://doi.org/10.3390/bdcc8120174>

- [17] Ying, Z., Wang, K., Xiong, J., & Ma, M. (2024). A literature review on V2X communications security: Foundation, solutions, status, and future. *IET communications*, 18(20), 1683–1715. <https://doi.org/10.1049/cmu2.12778>
- [18] Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity*, 2(1), 1–22. <https://doi.org/10.1186/s42400-019-0038-7>
- [19] Pethő, Z., Kazár, T. M., Szalay, Z., & Török, Á. (2024). Quantifying cyber risks: The impact of dos attacks on vehicle safety in V2X networks. *IEEE transactions on intelligent transportation systems*, 25(11), 18591–18600. <https://doi.org/10.1109/TITS.2024.3436840>
- [20] Sohail, M. S., Portomauro, G., Gaggero, G. B., Patrone, F., & Marchese, M. (2025). Performance analysis and security preservation of DSRC in V2X networks. *Electronics*, 14(19), 3786. <https://doi.org/10.3390/electronics14193786>
- [21] Fagan, M., Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020). *IoT device cybersecurity capability core baseline*. <https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf>
- [22] Zhao, C., Gill, J. S., Pisu, P., & Comert, G. (2021). Detection of false data injection attack in connected and automated vehicles via cloud-based sandboxing. *IEEE transactions on intelligent transportation systems*, 23(7), 9078–9088. <https://doi.org/10.1109/TITS.2021.3090361>
- [23] Yoshizawa, T., Singelée, D., Muehlberg, J. T., Delbruel, S., Taherkordi, A., Hughes, D., & Preneel, B. (2023). A survey of security and privacy issues in v2x communication systems. *ACM computing surveys*, 55(9), 1–36. <https://doi.org/10.1145/3558052>
- [24] McManus, I., & Heaslip, K. (2022). The impact of cyberattacks on efficient operations of CAVs. *Frontiers in future transportation*, 3, 792649. <https://doi.org/10.3389/ffutr.2022.792649>
- [25] Yin, L., Wang, Q., Shaw, S. L., Fang, Z., Hu, J., Tao, Y., & Wang, W. (2015). Re-identification risk versus data utility for aggregated mobility research using mobile phone location data. *PloS one*, 10(10), e0140589. <https://doi.org/10.1371/journal.pone.0140589>
- [26] Temoshok, D., Fenton, J., Choong, Y. Y., Lefkovitz, N., Regenscheid, A., & Richer, J. (2024). *Digital identity guidelines: authentication and authenticator management*. <https://doi.org/10.6028/NIST.SP.800-63B-4>
- [27] Force, J. T. (2020). *Security and privacy controls for information systems and organizations* (No. NIST Special Publication (SP) 800-53 Rev. 5 (Withdrawn)). National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>
- [28] Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine learning in IoT security: Current solutions and future challenges. *IEEE communications surveys & tutorials*, 22(3), 1686–1721. <https://doi.org/10.1109/COMST.2020.2986444>
- [29] Wang, C., Cheng, X., Li, J., He, Y., & Xiao, K. (2021). A survey: Applications of blockchain in the internet of vehicles. *EURASIP journal on wireless communications and networking*, 2021(1), 77. <https://doi.org/10.1186/s13638-021-01958-8>
- [30] Astarita, V., Giofrè, V. P., Mirabelli, G., & Solina, V. (2019). A review of blockchain-based systems in transportation. *Information*, 11(1), 21. <https://doi.org/10.3390/info11010021>
- [31] Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., ... & Zhao, S. (2021). Advances and open problems in federated learning. *Foundations and trends®in machine learning*, 14(1–2), 1–210. <https://www.nowpublishers.com/article/Details/MAL-083>
- [32] Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. *Foundations and trends®in theoretical computer science*, 9(3–4), 211–407. <https://doi.org/10.1561/04000000042>
- [33] Cheng, Y., Liu, Y., Chen, T., & Yang, Q. (2020). Federated learning for privacy-preserving AI. *Communications of the acm*, 63(12), 33–36. <https://doi.org/10.1145/3387107>
- [34] Bormann, C., Ersue, M., & Keranen, A. (2014). Terminology for constrained-node networks. *Internet engineering task force (IETF)*. <https://doi.org/10.17487/RFC7228>