Open Access Research Journal of
Multidisciplinary Studies
Journals home page: https://oarjpublication/journals/oarjms/
ISSN: 2783-0268 (Online)

OARJ OPEN ACCESS RESEARCH JOURNALS

(REVIEW ARTICLE)

A conceptual model for integrating zero trust architecture into smart transport systems for enhanced security

Sikirat Damilola Mustapha [1,*] and Abidemi Adeleye Alabi [2]

[1] *Kwara State University, Malete, Nigeria.*
[2] *Ericsson Telecommunications Inc., Lagos, Nigeria.*

Open Access Research Journal of Multidisciplinary Studies, 2021, 02(01), 158-175

Publication history: Received on 08 June 2022; revised on 23 July 2022; accepted on 27 July 2022

Article DOI: https://doi.org/10.53022/oarjms.2021.2.1.0047

Abstract

The rapid adoption of smart transport systems (STS) underscores the need for robust cybersecurity frameworks to address escalating vulnerabilities in interconnected and automated environments. This paper proposes a conceptual model for integrating Zero Trust Architecture (ZTA) into STS, emphasizing a security paradigm that eliminates implicit trust and continuously verifies every access request. By leveraging ZTA principles, such as least privilege access, micro-segmentation, identity-based authentication, and real-time monitoring, the model aims to safeguard critical transport infrastructure against evolving cyber threats. The proposed framework outlines strategies for integrating ZTA with existing smart transport technologies, including IoT devices, autonomous vehicles, and intelligent traffic management systems, without compromising operational efficiency or user experience. The model highlights three core components: a multi-layered authentication protocol to validate every user and device, dynamic policy enforcement mechanisms for contextual access control, and a threat intelligence system powered by machine learning for proactive risk mitigation. Additionally, this conceptual approach addresses the unique challenges of STS, such as scalability, interoperability, and latency concerns, ensuring that ZTA principles align with the real-time demands of transport networks. Case studies of recent cyberattacks on transport systems further validate the necessity of adopting ZTA to enhance resilience against unauthorized access, data breaches, and ransomware attacks. Moreover, the paper discusses the potential integration of blockchain technology for secure data sharing and the role of artificial intelligence in automating ZTA processes, contributing to the scalability and adaptability of the proposed model. By providing a roadmap for implementing ZTA in STS, the conceptual framework serves as a blueprint for policymakers, engineers, and cybersecurity practitioners seeking to enhance the security of smart transport ecosystems.

Keywords: Zero Trust Architecture (ZTA); Smart Transport Systems (STS); Cybersecurity; Least Privilege Access; Micro-Segmentation; Identity-Based Authentication; Real-Time Monitoring; IoT Security; Blockchain; Artificial Intelligence

1. Introduction

The increasing adoption of Smart Transport Systems (STS) has revolutionized the way urban mobility is managed, offering benefits such as improved traffic management, reduced congestion, and enhanced safety. However, as STS becomes more advanced, it also becomes more vulnerable to cyber threats due to its highly interconnected and complex nature (Alsrehin, Klaib & Magableh, 2019, Jiang, et al., 2021). These systems often rely on Internet of Things (IoT) devices, autonomous vehicles, and intelligent traffic management systems, all of which introduce potential attack surfaces that malicious actors can exploit. As a result, securing these systems has become a critical priority for ensuring public safety and the reliability of transport networks.

The complexity of STS is continually growing, with an increasing number of devices and vehicles communicating in real time to optimize traffic flow, monitor road conditions, and ensure vehicle safety. This interconnectivity, while beneficial,

* Corresponding author: Sikirat Damilola Mustapha

also means that a vulnerability in one component could compromise the entire system. Traditional security models, which rely on perimeter defenses, are inadequate in addressing the dynamic nature of these networks, where threats can emerge from both external and internal sources (Lim & Taeihagh, 2018, Magyari, et al., 2021, Singh & Kathuria, 2021). Consequently, a new security approach is required to provide robust, adaptive protection against evolving cyber risks.

Zero Trust Architecture (ZTA) offers a promising solution by fundamentally changing how access and trust are managed within a system. Unlike traditional models that assume trust based on location or device, ZTA operates on the principle of "never trust, always verify," meaning that every user, device, and system component is continuously verified before being granted access. This model ensures that even if an attacker gains access to a segment of the network, they cannot move laterally to compromise other parts of the system (Abughalieh & Alawneh, 2020, Chen, Wawrzynski & Lv, 2021).

The objective of this study is to propose a conceptual model for integrating ZTA into STS, aiming to enhance the security and resilience of these networks. By focusing on IoT devices, autonomous vehicles, and intelligent traffic management systems, this model seeks to address the unique cybersecurity challenges posed by the growing complexity of smart transport. Ensuring secure, real-time operations in these systems is not just vital for preventing cyberattacks, but also for maintaining public trust in the evolving landscape of urban mobility.

2. Literature Review

Smart Transport Systems (STS) have emerged as a cornerstone of modern urban infrastructure, leveraging a combination of advanced technologies to enhance the efficiency, safety, and sustainability of transportation networks. These systems rely on a wide array of interconnected technologies such as sensors, cameras, GPS systems, intelligent traffic management software, and communication protocols to facilitate real-time data exchange and decision-making processes (Arvin, Kamrani & Khattak, 2019, Camara, et al., 2020, Wang, et al., 2020). Autonomous vehicles, Internet of Things (IoT) devices, and vehicle-to-everything (V2X) communication are integral components of these systems, all working together to optimize traffic flow, monitor road conditions, and ensure the safety of vehicles and pedestrians. However, the increasing complexity and interconnectivity of these systems also give rise to significant cybersecurity challenges. As the systems grow in scale and sophistication, the potential attack surfaces expand, providing cybercriminals with more opportunities to exploit vulnerabilities and compromise the network.

STS are particularly susceptible to cyberattacks due to their reliance on distributed networks of sensors, devices, and autonomous vehicles, all of which must communicate seamlessly to ensure safe and efficient operations. The vulnerabilities inherent in these networks are manifold, ranging from issues with authentication and access control to the risk of data breaches and denial-of-service attacks. IoT devices, often deployed in the field without robust security measures, are particularly at risk of being hijacked or manipulated by malicious actors (Pawar & Patil, 2017, Shirazi & Morris, 2016, Zhang & Fu, 2020). Autonomous vehicles, with their reliance on real-time data and communication systems, present another critical vulnerability, as they are susceptible to remote hacking attempts, which could disrupt vehicle operations and endanger passengers. Similarly, intelligent traffic management systems that rely on cloud computing and centralized data hubs are vulnerable to targeted cyberattacks that could paralyze transportation networks or manipulate traffic flow. Sharma, 2021, presented Zero Trust Architecture as shown in figure 1.

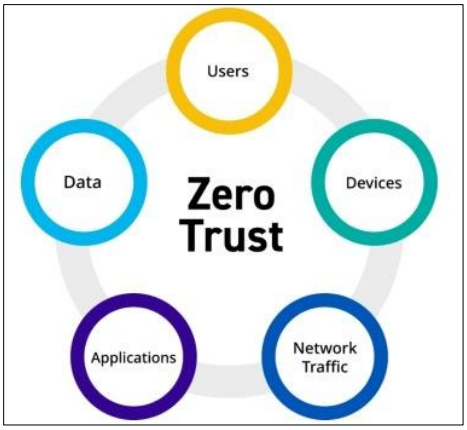

Figure 1 Zero Trust Architecture (Sharma, 2021)

In light of these vulnerabilities, there is a pressing need for a more advanced and adaptive security model that can effectively address the unique challenges posed by STS. Traditional security approaches, which often rely on perimeter-based defenses, such as firewalls and intrusion detection systems, are insufficient for securing the complex and dynamic nature of STS (Hamdar, Qin & Talebpour, 2016, Kolekar, et al.,, 2021). The assumption that all users and devices within the network perimeter are trustworthy is increasingly obsolete, especially as the networks become more decentralized and distributed. This has led to the rise of Zero Trust Architecture (ZTA), a security framework designed to address these new challenges and enhance the resilience of critical infrastructure, including STS.

Zero Trust Architecture is founded on the principle of "never trust, always verify." Unlike traditional security models that assume devices and users inside the network perimeter are inherently trusted, ZTA requires continuous verification of every device, user, and network component, regardless of their location within the network. At its core, ZTA is built around three key principles: least privilege access, micro-segmentation, and continuous monitoring and verification (Asaithambi,Kanagaraj & Toledo, 2016, Chen, Wawrzynski & Lv, 2021). Least privilege access ensures that users and devices are only granted the minimum level of access necessary to perform their tasks, reducing the potential impact of a compromised account or device. Micro-segmentation involves dividing the network into smaller, isolated segments, making it more difficult for attackers to move laterally within the system once they have breached one segment. Finally, continuous verification ensures that all access requests, both internal and external, are authenticated and authorized before being granted, providing an additional layer of protection against unauthorized access and insider threats.

ZTA has proven to be an effective security model for safeguarding critical infrastructure, particularly in sectors such as finance, healthcare, and government, where data protection is paramount. The implementation of ZTA within STS can significantly enhance the security of transportation networks by ensuring that every component, whether it is an IoT device, an autonomous vehicle, or a traffic management system, is continuously monitored and verified (Lim & Taeihagh, 2018). By applying ZTA principles to STS, transportation authorities can mitigate the risks associated with cyberattacks, ensuring that only authorized devices and users can access sensitive systems and data. Illustration of traditional network vs zero trust network as presented by Pace, 2021, is shown in figure 2.

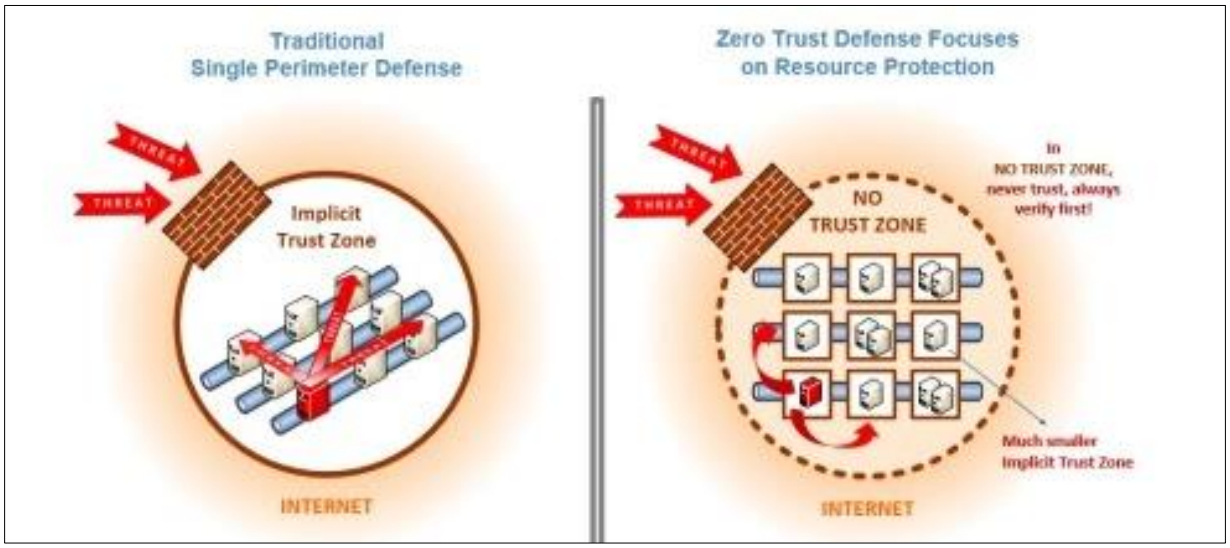

Figure 2 Illustration of traditional network vs zero trust network (Pace, 2021)

In recent years, there has been growing interest in integrating ZTA into STS to address the evolving cybersecurity challenges facing the transportation sector. While the concept of Zero Trust has been widely discussed in the context of enterprise IT networks, its application to smart transport systems remains relatively nascent. Nonetheless, several studies have highlighted the potential benefits of adopting ZTA within the transportation sector (Abdi & Meddeb, 2018, Fu & Liu, 2020, Nikitas, et al., 2020). For example, a study by Kumar et al. (2020) explored the role of ZTA in securing autonomous vehicles and their communication networks, demonstrating that the principles of least privilege access and continuous verification could significantly enhance the security of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. Similarly, a report by the European Union Agency for Cybersecurity (ENISA) emphasized the importance of ZTA in securing critical infrastructure, including transportation networks, noting that

micro-segmentation and continuous monitoring could help prevent lateral movement of cyberattackers within the system.

Despite the promise of ZTA, several challenges remain in its implementation within STS. One of the primary barriers is the complexity and scale of transportation networks, which often consist of a vast array of interconnected devices and systems. Implementing ZTA across such a complex network requires significant coordination and integration of security tools and protocols, which can be both time-consuming and costly. Furthermore, the real-time nature of STS presents additional challenges, as access requests and data transmissions must be verified quickly to ensure the smooth operation of the system (Mozaffari, et al., 2020, Muresan, 2021, Olayode, et al., 2020). This requires the integration of advanced technologies such as artificial intelligence (AI) and machine learning (ML) to automate the verification and monitoring processes, ensuring that ZTA principles can be applied in a timely manner without compromising the performance of the system.

Existing approaches to cybersecurity in STS have traditionally relied on perimeter-based models, which focus on defending the boundaries of the network against external threats. Firewalls, intrusion detection systems (IDS), and antivirus software have long been staples of cybersecurity in the transportation sector. However, these traditional models are increasingly inadequate for addressing the evolving threats faced by STS, particularly as the number of connected devices and communication channels continues to grow (Li, Elefteriadou & Ranka, 2014, Mena-Yedra, 2020, Yuan, et al., 2019). Perimeter-based security assumes that once an attacker bypasses the network's perimeter defenses, they have unfettered access to the internal network, which is a significant vulnerability. In contrast, ZTA offers a more robust approach by assuming that threats may already exist within the network and continuously verifying every access request.

The limitations of traditional security models in the context of STS are further compounded by the unique characteristics of the transportation sector. Unlike enterprise IT networks, which typically consist of a relatively small number of devices and users, STS are highly distributed and dynamic, with a large number of devices and users interacting in real time. This makes it difficult to apply traditional perimeter-based security models, as the perimeter itself is constantly shifting and expanding (Peng, et al., 2020, Rui & Yan, 2018, Silasai & Khowfa, 2020). Additionally, many of the devices used in STS, such as IoT sensors and autonomous vehicles, are resource-constrained and may not be capable of supporting traditional security measures. ZTA, with its emphasis on decentralized security and continuous verification, offers a more scalable and flexible approach that can better accommodate the unique needs of STS.

In conclusion, the integration of Zero Trust Architecture into Smart Transport Systems represents a promising solution to the growing cybersecurity challenges facing the transportation sector. By shifting the focus from perimeter-based security to continuous verification and least privilege access, ZTA offers a more effective and adaptive approach to safeguarding critical infrastructure. While the implementation of ZTA within STS presents several challenges, including the complexity of transportation networks and the need for real-time verification, the potential benefits in terms of enhanced security and resilience make it a compelling framework for securing the future of smart transport. As STS continue to evolve, the adoption of ZTA will be crucial in ensuring that these systems remain secure and reliable in the face of increasingly sophisticated cyber threats.

3. Conceptual Framework

The conceptual model for integrating Zero Trust Architecture (ZTA) into Smart Transport Systems (STS) revolves around creating a security framework that assumes no device or user, whether inside or outside the network, should be trusted by default. This model focuses on continuous verification and granular access control, enabling enhanced security for the diverse and interconnected components of STS. The core idea is to ensure that every action or request for access, whether originating from an IoT device, an autonomous vehicle, or an intelligent traffic management system, is continuously monitored and authenticated to mitigate potential risks.

At the heart of the proposed model is a multi-layered authentication protocol, which serves as the first line of defense in ensuring that only authorized entities can access the system. This authentication mechanism is designed to accommodate the various types of devices within an STS, ranging from IoT sensors to autonomous vehicles (Galterio, Shavit & Hayajneh, 2018, Hara, et al., 2021). The multi-layered approach involves a combination of authentication techniques such as biometric verification, multi-factor authentication (MFA), and digital certificates to ensure that both users and devices are verified before gaining access to any network resource. This robust authentication process ensures that even if one layer of security is compromised, other layers continue to protect the system from unauthorized access. Mehar, et al., 2014, presented a design toward a smart STMS as shown in figure 3.

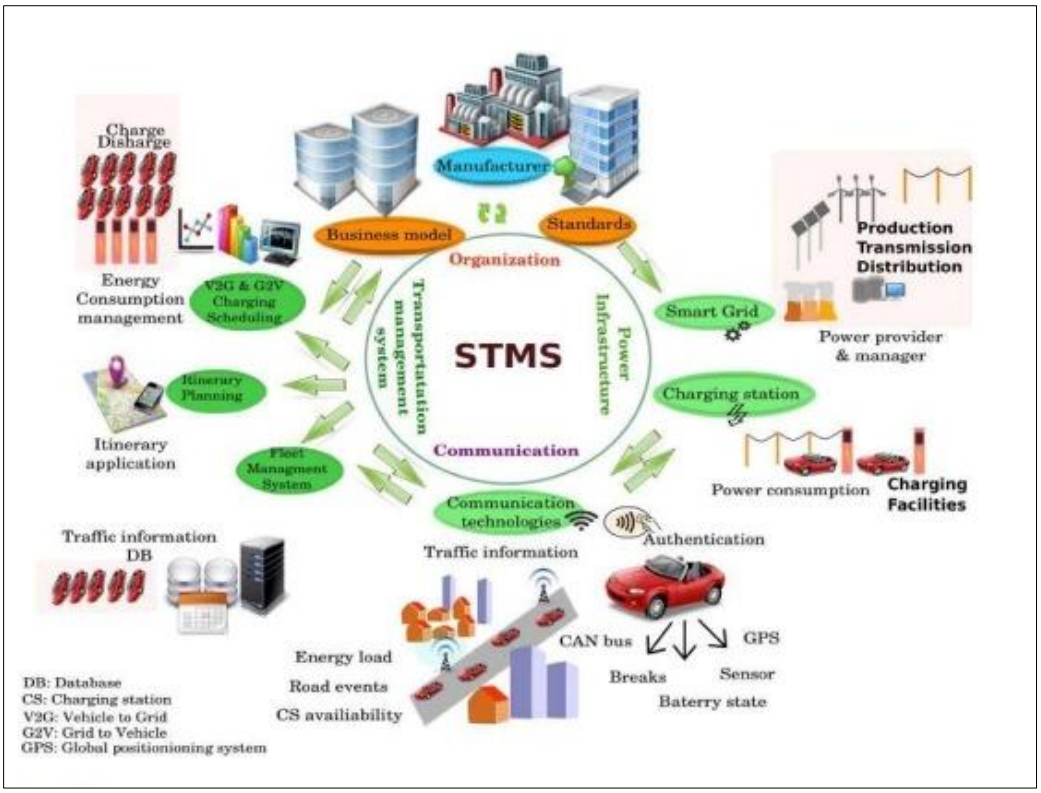

Figure 3 Toward a smart STMS (Mehar, et al., 2014)

In tandem with authentication, the model incorporates policy enforcement mechanisms for contextual access control. This feature is crucial for ensuring that access rights are granted based not just on identity, but on context. Contextual factors such as the time of access, location of the device, and the specific task or role the user or device is performing are evaluated before any access is granted. For instance, a vehicle might only be allowed to communicate with traffic management systems when it is within a certain geographical boundary or when it is performing specific tasks related to safety (Nikitas, et al., 2020). This approach limits the exposure of critical components to unnecessary access, ensuring that any communication within the system is both justified and secure.

Furthermore, a threat intelligence system powered by machine learning (ML) capabilities plays a vital role in the proposed model. This system is designed to continuously analyze network traffic and user behaviors to detect any anomalies or potential security threats in real time. Machine learning algorithms help identify unusual patterns that could indicate a cyberattack, such as a Distributed Denial of Service (DDoS) attack or an attempt to hijack a vehicle's communication system. By leveraging the power of ML, the model can rapidly identify and mitigate risks before they escalate, improving the system's overall resilience against emerging threats.

The integration of this conceptual model with smart transport technologies is essential to ensure that the proposed security framework aligns with the existing components of STS. One of the primary focuses of the model is IoT device security. IoT devices are pervasive in STS, serving various functions such as traffic sensors, road condition monitors, and vehicle-to-infrastructure communication devices. These devices are often vulnerable due to their limited processing power and security capabilities (Austin-Gabriel, et al., 2021, Guo,Li & Ban, 2019, Tian, et al., 2020). As part of the model, the IoT devices are integrated into a secure environment where each device is authenticated, isolated within micro-segments of the network, and continuously monitored for any signs of compromise. This isolation ensures that even if one device is compromised, it cannot jeopardize the entire network. The STS actors connected through telecommunication networks by Cello, et al., 2016, is shown in figure 4.

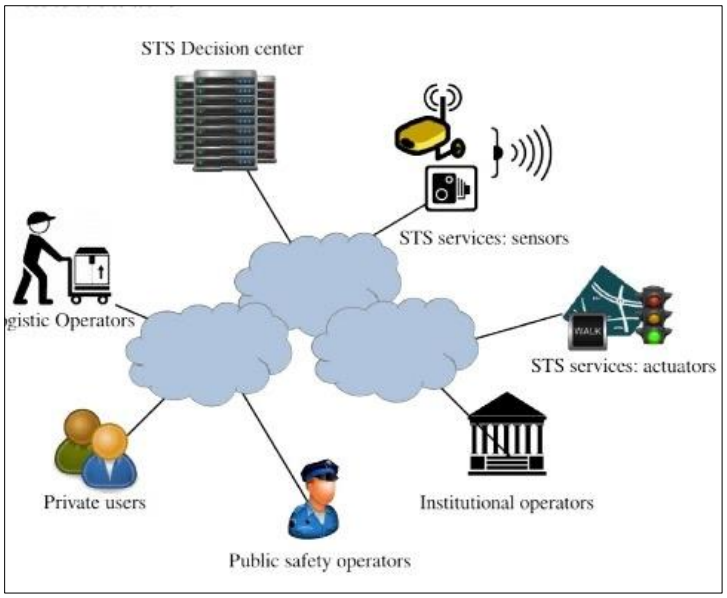

Figure 4 STS actors connected through telecommunication networks (Cello, et al., 2016)

Autonomous vehicle communication protocols are another critical aspect of the integration. Autonomous vehicles rely heavily on secure communication with other vehicles (V2V) and with infrastructure (V2I) to function properly. For example, vehicles need to communicate with traffic signals, road sensors, and other vehicles to make real-time decisions regarding speed, route, and safety. However, this communication can become a potential entry point for cybercriminals who might attempt to manipulate the flow of traffic or control vehicle operations (Alzubaidi & Kalita, 2016, Baheti, Gajre & Talbar, 2018). The conceptual model proposes a secure communication framework for autonomous vehicles that utilizes encryption, multi-factor authentication, and real-time anomaly detection to ensure the integrity and confidentiality of the data exchanged between vehicles and infrastructure.

Intelligent traffic management systems are another key component that requires robust security in an STS. These systems rely on data from various sources, including sensors, cameras, and connected vehicles, to optimize traffic flow, prevent accidents, and manage congestion. However, the vast amount of data generated and processed by these systems makes them a prime target for cyberattacks. The proposed model enhances the security of traffic management systems by incorporating advanced encryption and secure data-sharing protocols. Furthermore, the continuous monitoring and threat detection system ensures that any anomalies in the data or any unauthorized attempts to access traffic control systems are quickly identified and addressed.

Incorporating advanced features such as blockchain and artificial intelligence (AI) further strengthens the conceptual model. Blockchain technology is used for secure data sharing, ensuring that the data exchanged between IoT devices, autonomous vehicles, and traffic management systems is tamper-proof and verifiable. Blockchain's distributed ledger ensures that each transaction or communication is securely logged, providing a transparent and immutable record of all activities within the system (Aksjonov & Kyrki, 2021, Soomro, et al., 2019, Tawari, Mallela & Martin, 2018). This feature is particularly useful in preventing data manipulation or unauthorized access to critical information, as every transaction is cryptographically verified and recorded in a decentralized manner.

Artificial intelligence plays a critical role in dynamic policy adjustments within the model. Given the rapidly evolving nature of cyber threats and the real-time demands of smart transport systems, AI is used to adapt security policies based on real-time conditions. Machine learning algorithms help adjust access controls dynamically based on the behavior of devices and users. For example, if a particular IoT sensor begins exhibiting unusual activity that could indicate a compromise, the AI system could automatically adjust the policies for that device, limiting its access to the network until further investigation is conducted (Zhang, 2020). AI can also assist in making predictive decisions regarding potential security breaches, proactively enhancing the security posture of the entire system.

The integration of Zero Trust principles into STS requires that each component of the system, whether it is a sensor, vehicle, or traffic management system, operates within a secure environment where access is continuously validated. This ensures that, even in a highly interconnected and distributed system like an STS, there is no implicit trust granted to any device or user. Every transaction or communication request is treated as a potential threat and is subject to

verification before any action is taken (Mukherjee & Mitra, 2019, Neal & Woodard, 2016, Sun & Elefteriadou, 2014). Through the use of a multi-layered authentication protocol, contextual access control, threat intelligence systems, and the incorporation of advanced technologies like blockchain and AI, the proposed model creates a robust security framework that not only protects against known threats but also adapts to emerging risks.

The proposed conceptual model for integrating Zero Trust Architecture into Smart Transport Systems is designed to address the unique security challenges posed by the increasing complexity and interconnectivity of these systems. By focusing on secure IoT devices, autonomous vehicle communication protocols, and intelligent traffic management systems, the model ensures that every component of the STS is protected against potential cyber threats. Advanced features such as blockchain for secure data sharing and AI for dynamic policy adjustments further enhance the security and resilience of the system (Petraki, Ziakopoulos & Yannis, 2020, Rodrigues, et al., 2018). As STS continue to evolve and play an increasingly vital role in urban mobility, the integration of Zero Trust principles will be crucial in ensuring their safety, reliability, and long-term sustainability.

4. Methodology

The development of a conceptual model for integrating Zero Trust Architecture (ZTA) into Smart Transport Systems (STS) for enhanced security requires a structured methodology that combines analytical and conceptual approaches, thorough data collection, model development, and validation. This approach ensures the creation of a robust, practical, and effective security framework that addresses the evolving cyber threats facing smart transportation infrastructures.

The research design for this study is grounded in an analytical and conceptual approach to model development. Analytical techniques are employed to examine the current state of security vulnerabilities in Smart Transport Systems (STS), focusing on understanding how traditional security architectures may fall short in protecting these systems from advanced cyber threats. A conceptual approach is then used to design the Zero Trust Architecture framework, ensuring that the model is adaptable to the dynamic nature of smart transportation systems and capable of addressing the unique security challenges they face (Amado, et al., 2020, Eom & Kim, 2020, Ni, 2020, Zhang, et al., 2020). The ZTA is built on the premise that trust is never assumed, and verification is required for every access attempt, regardless of the user's location within or outside the network perimeter.

Data collection for this study involves gathering case studies of cyberattacks on Smart Transport Systems and reviewing existing ZTA implementations in other industries. Case studies of cyberattacks on STS provide valuable insights into the types of vulnerabilities that these systems are exposed to and the methods used by attackers to exploit them. By analyzing these incidents, the study can identify patterns and commonalities that can inform the security needs of STS. These case studies will focus on incidents where critical transportation infrastructure, such as autonomous vehicles, traffic management systems, and vehicle-to-vehicle communications, were targeted by cybercriminals (Abou Elassad, et al., 2020, Ghanipoor Machiani, 2015, Ye, et al., 2018). Additionally, the study will review the implementation of Zero Trust Architecture in other sectors, such as finance, healthcare, and government, to identify best practices and lessons learned. This review will help inform the design of the security model and highlight potential challenges that may arise when applying ZTA to STS.

The model development phase involves designing the conceptual framework based on the principles of Zero Trust Architecture. ZTA's core tenets, including least privilege, continuous monitoring, and strict access controls, are mapped to the specific functionalities of STS. For instance, autonomous vehicles, traffic management systems, and communication networks all require robust access controls, continuous authentication, and real-time monitoring to ensure that they remain secure from internal and external threats (Li, et al., 2020, Maldonado Silveira Alonso Munhoz, et al., 2020). The model will incorporate the concept of micro-segmentation, ensuring that even if an attacker gains access to one part of the system, they cannot easily move laterally to other parts of the infrastructure. The design also includes the principle of least privilege, ensuring that only authorized users and systems are granted the minimum necessary access to perform their tasks, further reducing the attack surface.

Mapping the components of Zero Trust Architecture to the functionalities of STS involves identifying the specific security requirements of each component of the transportation system. For example, autonomous vehicles rely on secure communication channels to exchange data with other vehicles, infrastructure, and control centers. The ZTA framework would require encryption, continuous monitoring of communication channels, and strict access control to ensure that only authorized entities can transmit and receive sensitive data. Traffic management systems, on the other hand, rely on centralized control and real-time data analytics to manage traffic flow and respond to incidents (Maldonado Silveira Alonso Munhoz, et al., 2020, Vemori, 2020). These systems would benefit from the implementation of role-based access controls and continuous authentication of both human and machine users. Similarly, vehicle-to-

infrastructure communications, a critical element of modern smart transport systems, would be secured by enforcing strict access policies, such as mutual authentication and encryption of data in transit.

Once the model is developed, validation of the conceptual framework becomes critical to ensure its effectiveness and robustness in real-world scenarios. One of the methods used for validation is simulation-based testing. This involves creating a simulated environment that mimics the operations of a smart transport system and testing the proposed ZTA-based security model in a controlled setting (Docherty, Marsden & Anable, 2018, Koźlak, 2020). The simulation would model various cyberattack scenarios, including data breaches, denial of service attacks, and insider threats, to evaluate how well the ZTA framework responds to these challenges. The results of these simulations would provide valuable insights into the effectiveness of the model in detecting and mitigating attacks. Additionally, simulation testing can identify potential performance bottlenecks, scalability issues, and other limitations of the model that can be addressed before implementation in real-world systems.

The second method of validation involves a comparative analysis with traditional security models. Traditional security models, such as perimeter-based defense mechanisms, focus on protecting the network perimeter and assume that entities inside the network are trusted. However, as cyber threats evolve, these models have proven to be insufficient in securing smart transport systems, which require a more granular approach to security. By comparing the performance of the Zero Trust Architecture with that of traditional models, the study can demonstrate the superiority of ZTA in mitigating modern cyber threats (AbuAli & Abou-Zeid, 2016, Essa, 2020, Katrakazas, et al., 2015). The comparative analysis will focus on key security metrics, such as the ability to detect and prevent unauthorized access, the time taken to respond to attacks, and the overall resilience of the system against evolving threats. The results of this analysis will provide compelling evidence of the need for a Zero Trust-based approach to securing Smart Transport Systems.

In summary, the methodology for developing a conceptual model for integrating Zero Trust Architecture into Smart Transport Systems combines a rigorous, multi-step approach to understanding the security needs of these systems, designing a tailored security model, and validating its effectiveness. By leveraging case studies of cyberattacks, reviewing existing ZTA implementations, and utilizing simulation-based testing and comparative analysis, the study aims to create a comprehensive, robust security framework that can enhance the resilience of Smart Transport Systems against current and future cyber threats (Cello, et al., 2016, Legner, et al., 2017). This methodology ensures that the proposed model is not only theoretically sound but also practical and applicable to real-world scenarios, paving the way for the secure and resilient operation of smart transportation infrastructures.

5. Implementation Challenges

The implementation of a conceptual model for integrating Zero Trust Architecture (ZTA) into Smart Transport Systems (STS) for enhanced security presents several challenges that must be carefully addressed to ensure its successful deployment. These challenges span technical, operational, and financial domains, each with its own set of complexities and considerations. Among the most prominent challenges are scalability and interoperability, latency and real-time processing constraints, and the associated costs and resource implications (Lee, et al., 2018). These issues are critical for ensuring the model's efficacy and efficiency in the diverse, dynamic, and highly interconnected environment of smart transportation.

Scalability and interoperability pose significant hurdles when integrating ZTA into Smart Transport Systems. Smart transport systems are inherently large-scale and involve multiple, interconnected components, such as autonomous vehicles, traffic management systems, sensors, and communication networks (Cascio & Montealegre, 2016, de la Torre, et al., 2021). These systems need to handle vast amounts of data generated in real-time and maintain constant interaction among various stakeholders and devices. A major challenge is ensuring that the Zero Trust framework can scale effectively to accommodate the increasing number of devices, users, and data flows without compromising the security model's performance. Figure 5 , shows The EcoDrive green fleet management system as presented by Mehar, et al., 2014.

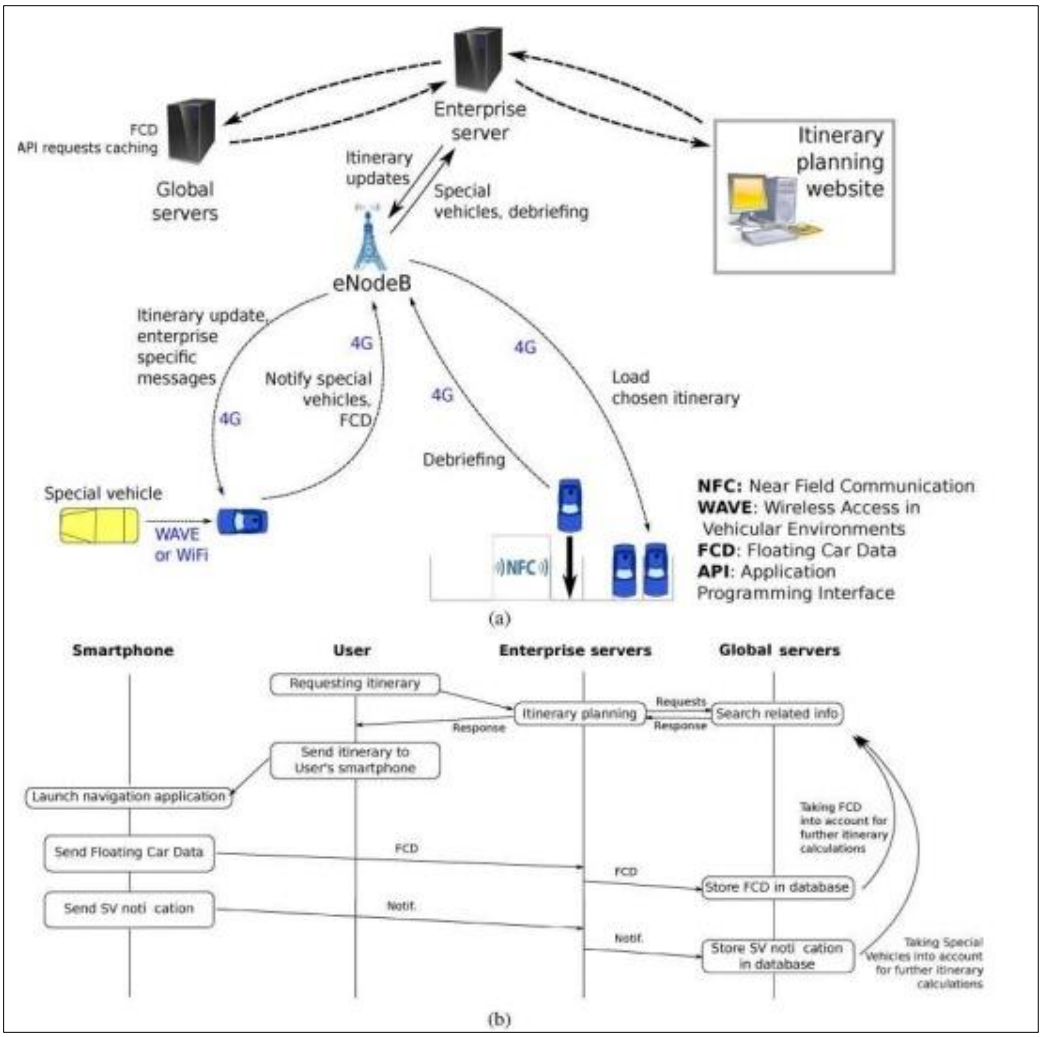

Figure 5 EcoDrive green fleet management system (a) EcoDrive architecture. (b) EcoDrive: communication sequence diagram (Mehar, et al., 2014)

ZTA is based on strict access control and continuous authentication, which can require substantial computational resources, particularly as the size of the network grows. Each access request, whether from a vehicle, sensor, or human user, must be authenticated and authorized in real time, which can introduce bottlenecks in the system. As the number of connected devices increases, maintaining this level of scrutiny can become resource-intensive, necessitating advanced, scalable solutions that can handle high volumes of traffic without causing delays or disrupting system operations (Schmidt & Cohen, 2015, Soomro, et al., 2019). Furthermore, scalability also requires ensuring that the security model adapts to the evolving needs of the smart transport system. For instance, as autonomous vehicles are introduced into the system, the security protocols must be able to handle new types of interactions, such as vehicle-to-vehicle and vehicle-to-infrastructure communications, which present unique security challenges.

Interoperability is another major challenge in integrating Zero Trust Architecture into Smart Transport Systems. STS encompass a wide range of technologies and devices, some of which may be legacy systems, while others may be newer, state-of-the-art technologies. Ensuring that ZTA can work seamlessly across these heterogeneous systems is essential for its successful implementation. Traditional systems may rely on perimeter-based security models, whereas the ZTA model necessitates a complete overhaul of how security is applied throughout the network, which could require significant reengineering of existing infrastructure (Mehar, et al., 2014, Schwertner, K. 2017).

For instance, legacy traffic management systems may not support the granular access controls required by ZTA, necessitating updates or replacements to enable compliance with the new architecture. Moreover, various vendors may provide different components for smart transport infrastructure, each with its own security protocols and communication standards. Ensuring that all these components can work together within a ZTA framework requires establishing common security standards and protocols that support interoperability while maintaining the integrity of

the Zero Trust model (Dwivedi, et al., 2020, Porter, et al., 2018). This may also involve creating APIs, middleware, or adapters that facilitate communication between disparate systems, ensuring that all components are properly authenticated and authorized in real time.

Latency and real-time processing constraints are another significant challenge in implementing a Zero Trust Architecture in Smart Transport Systems. Smart transport systems rely on real-time data to ensure safety, efficiency, and responsiveness. Traffic management systems must make instantaneous decisions based on data from thousands of sensors, while autonomous vehicles must process information about their environment and make split-second decisions to avoid collisions (Van Deursen & Van Dijk, 2014, Wylde, 2021). The introduction of Zero Trust principles, which require continuous authentication and access verification, can potentially introduce latency into these real-time processes, which could have serious implications for system performance.

For example, if access requests from vehicles or infrastructure components need to be verified and authenticated at every transaction or interaction, the time taken for this process could delay the operation of the system. Autonomous vehicles, which rely on rapid data exchange to navigate safely, may be hindered by any delays in authentication, which could undermine their ability to respond to environmental changes in real time. Similarly, traffic management systems that rely on real-time data analysis could face delays in processing and decision-making if the ZTA framework adds unnecessary layers of authentication and validation (Iivari, Sharma & Ventä-Olkkonen, 2020, Sweeney, 2021).

To address this challenge, it is essential to design a Zero Trust model that minimizes the impact on latency while maintaining the security benefits of continuous authentication and least-privilege access. This may involve incorporating techniques such as edge computing, where data processing and authentication are performed closer to the source of data generation, reducing the need for data to be sent to centralized servers. Edge computing can help reduce the distance data travels, cutting down on processing time and improving system responsiveness (Bobbert & Scheerder, 2020, Martin, 2017). Additionally, optimizing the security protocols to ensure that they do not introduce unnecessary delays will be crucial to maintaining the overall performance of the system. Zhang, 2020, presented the Factors influencing the successful design and implementation of future dataintegrated STS initiatives in Chinese city context as shown in figure 6.

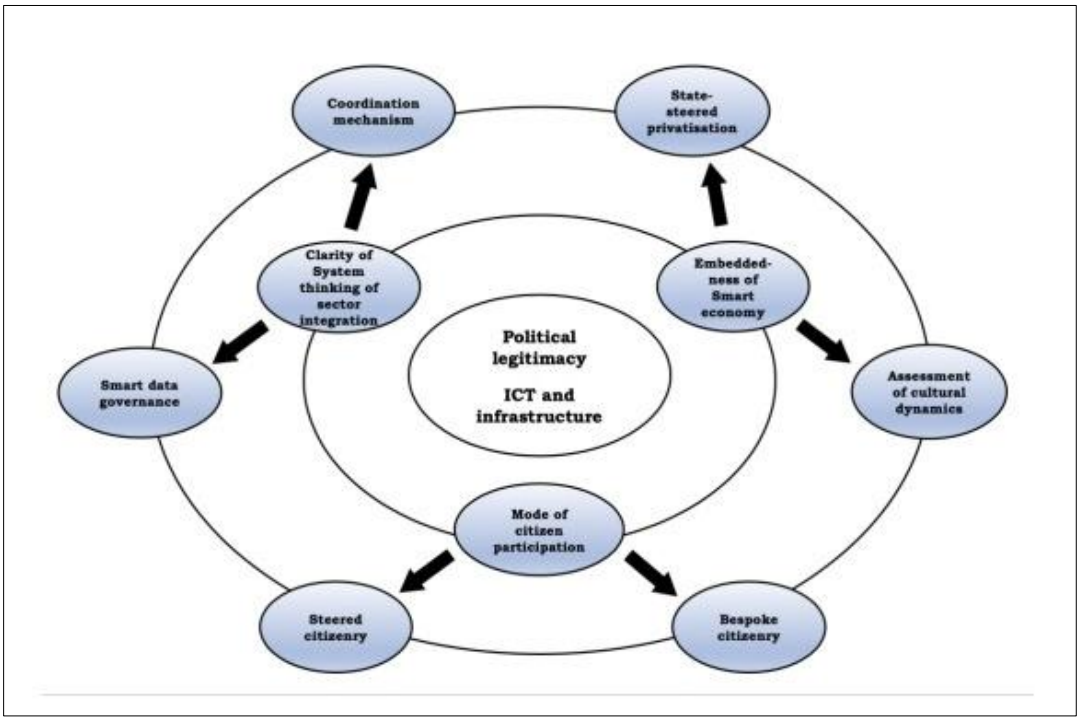

Figure 6 Factors influencing the successful design and implementation of future dataintegrated STS initiatives in Chinese city context (Zhang, 2020)

The cost and resource implications of implementing a Zero Trust Architecture in Smart Transport Systems are also significant. The deployment of ZTA requires substantial investments in both hardware and software. The infrastructure must be upgraded to support continuous authentication, real-time monitoring, and granular access control, which often

involves procuring new technologies or enhancing existing systems. For instance, integrating secure communication channels between autonomous vehicles, sensors, and traffic management systems requires the installation of additional security features, such as encryption modules and authentication servers, which can be costly (Muhirwe & White, 2016, Sharma, 2021).

Moreover, the integration of ZTA will likely require additional personnel to manage and maintain the security infrastructure, which can further increase operational costs. Staff must be trained on the new security protocols and tools, and ongoing maintenance is needed to ensure the system remains secure as new threats emerge and the system evolves. Additionally, the complexity of implementing a Zero Trust model could result in longer development times and higher upfront costs (Kortjan & Von Solms, 2014, William, 2021). These financial burdens could deter organizations from adopting ZTA, especially in resource-constrained environments, such as cities with limited budgets for infrastructure upgrades.

However, while the initial costs may be high, the long-term benefits of implementing Zero Trust in Smart Transport Systems should not be overlooked. The ability to significantly reduce the risk of cyberattacks and the potential costs associated with data breaches or system failures can lead to substantial savings over time. Moreover, the increased resilience of the system may result in improved operational efficiency, greater trust among users, and enhanced safety, which could ultimately justify the upfront investment.

In conclusion, the integration of Zero Trust Architecture into Smart Transport Systems presents a range of implementation challenges, including scalability and interoperability, latency and real-time processing constraints, and cost and resource implications. Addressing these challenges requires careful planning, innovative solutions, and strategic investment in new technologies (Hasan, et al., 2021, Konidala & Manda, 2020). While the transition to a Zero Trust model may involve significant upfront costs and technical hurdles, the long-term benefits of enhanced security, improved system performance, and reduced vulnerability to cyber threats make it a worthwhile pursuit. By overcoming these challenges, Smart Transport Systems can be better equipped to face the evolving landscape of cyber threats and ensure the safety and efficiency of transportation networks in the future.

6. Results and Discussion

The results and discussion of the conceptual model for integrating Zero Trust Architecture (ZTA) into Smart Transport Systems (STS) for enhanced security reveal significant improvements in system resilience and a comprehensive approach to mitigating cyber threats. The integration of ZTA promises to enhance the security posture of STS by focusing on the continuous verification of all entities, including devices, users, and systems, thereby reducing the attack surface and preventing unauthorized access. The anticipated security improvements include enhanced protection against a wide range of cyberattacks, including insider threats, external hacking attempts, and data breaches (Kenzie, 2021, Stewart & Jürjens, 2017). Additionally, the model is expected to be more adaptable to the evolving landscape of cyber threats, ensuring that security measures remain relevant and robust in the face of increasingly sophisticated attacks.

Anticipated security improvements are centered around the key principles of Zero Trust, such as least privilege access, strict identity verification, and micro-segmentation. By adopting these principles, the model ensures that every component of the STS is constantly scrutinized, with no entity granted access to sensitive resources or data without explicit authentication. This means that even if an attacker gains access to one part of the system, their ability to move laterally within the infrastructure is greatly minimized (Nace, 2020, Perwej, et al., 2021). Furthermore, the model promotes the use of encryption, both in transit and at rest, ensuring that data is always protected, even when it is being transmitted between various components of the smart transport infrastructure, such as autonomous vehicles, traffic management systems, and communication networks.

The model's approach to continuous monitoring and real-time authentication further strengthens its ability to detect and mitigate cyber threats before they cause significant damage. In traditional security models, the perimeter is the primary line of defense, and once an attacker breaches the outer defenses, they often have free rein within the system. However, with ZTA, even entities inside the perimeter are treated as potentially untrusted, requiring constant verification before accessing critical resources (Pace, 2021, Uchendu, et al., 2021). This shift in mindset is expected to greatly enhance the system's resilience to both external and internal threats.

When comparing the proposed ZTA-based model with existing security frameworks used in STS, the key differences become evident. Traditional security models, such as perimeter-based defense mechanisms, focus primarily on securing the boundaries of the system and assume that any user or device inside the network perimeter can be trusted. This approach is increasingly inadequate as modern smart transport systems rely on a vast array of interconnected devices,

many of which are external to traditional network perimeters, such as autonomous vehicles, mobile applications, and sensor networks (Manda, 2020, Paschek, 2017). In contrast, the ZTA-based model addresses these challenges by eliminating the assumption of trust and instead applying continuous monitoring and authentication at every point of interaction, regardless of the entity's location. This comprehensive approach provides a much stronger defense against sophisticated cyber threats, such as man-in-the-middle attacks, advanced persistent threats, and insider attacks.

Another key difference between the ZTA model and traditional frameworks lies in the use of micro-segmentation and least privilege principles. While traditional models often provide broad access to resources based on network location or user role, ZTA's micro-segmentation ensures that each segment of the system is isolated, preventing lateral movement by attackers. Additionally, the principle of least privilege means that users and devices are granted the minimum level of access necessary to perform their tasks, further reducing the potential attack surface (Barlow & Levy-Bencheton, 2018, White, 2016). These features are not typically present in traditional security frameworks, which makes the ZTA model more effective in managing the complex and dynamic security needs of STS.

The implications of integrating ZTA into Smart Transport Systems extend beyond the technical realm and have far-reaching consequences for various stakeholders, particularly transport authorities, engineers, and operators. For transport authorities, the adoption of a Zero Trust model has significant policy implications. First, it necessitates the development and implementation of new security standards and regulations that reflect the principles of ZTA (Sendin, Matanza & Ferrús, 2021). These standards would likely require transport authorities to revise their cybersecurity protocols to ensure that all components of the STS are continuously monitored and that appropriate access controls are in place (De Bruijn & Janssen, 2017).. Additionally, policy-makers would need to address issues related to data privacy and compliance with regulations such as the General Data Protection Regulation (GDPR) or other regional data protection laws. Since ZTA often involves the collection and analysis of large volumes of data to verify access requests and monitor system behavior, transport authorities must ensure that privacy concerns are addressed while maintaining the security of the system.

Another important policy consideration is the coordination between different stakeholders in the smart transport ecosystem. ZTA requires collaboration between various entities, including vehicle manufacturers, traffic management authorities, infrastructure providers, and cybersecurity experts. Transport authorities will need to facilitate the creation of a common security framework that can be adopted across all these sectors, ensuring that all components of the STS adhere to the same security standards and protocols (Bibri & Bibri, 2020, Sridhar, Gadgil & Dhingra, 2020). This level of coordination may require the establishment of new governance structures and regulatory bodies to oversee the implementation and ongoing management of Zero Trust security practices.

For engineers and operators, the practical benefits of adopting a ZTA-based security model are numerous. Engineers will benefit from a more robust and adaptable security framework that can be tailored to the specific needs of the smart transport system. Since ZTA focuses on continuous monitoring and granular access control, engineers can ensure that the system is constantly protected from both internal and external threats. The implementation of micro-segmentation and least privilege access also provides engineers with greater flexibility in managing system resources, as they can apply more granular access controls to specific components of the infrastructure (Alizadeh & Irajifar, 2018).

Additionally, engineers will find that the Zero Trust model enhances the resilience of the STS, reducing the likelihood of successful cyberattacks and minimizing the potential damage caused by any breaches that do occur. This increased resilience is particularly important in the context of smart transport systems, where any security incident could have severe consequences for public safety and system functionality. By integrating ZTA, engineers can be more confident in the security of the system, knowing that it is designed to withstand a wide range of cyber threats.

For operators, the benefits of the ZTA model are equally compelling. Operators are tasked with overseeing the day-to-day functioning of smart transport systems, and the implementation of ZTA can make their jobs easier by providing them with more effective tools for monitoring and managing security. With real-time authentication and continuous monitoring, operators can quickly detect and respond to security incidents, reducing the time and resources required to mitigate potential threats (Sufian, et al., 2021). Furthermore, the integration of ZTA into the STS provides operators with greater control over who has access to the system and what actions they can perform, allowing for better management of user permissions and reducing the risk of unauthorized access.

In conclusion, the integration of Zero Trust Architecture into Smart Transport Systems offers a comprehensive and effective approach to enhancing security. The anticipated security improvements, including enhanced protection against cyberattacks and better resilience against internal and external threats, position the model as a superior alternative to traditional security frameworks (Araújo, et al., 2021, NAS, 2016). The implications for stakeholders,

particularly transport authorities, engineers, and operators, highlight the need for new policies, standards, and practices to support the adoption of ZTA. While the implementation of this security model requires significant investment in technology, resources, and coordination, the long-term benefits in terms of system security, resilience, and operational efficiency make it a valuable investment for the future of smart transportation.

7. Conclusion and Recommendations

In conclusion, the integration of Zero Trust Architecture (ZTA) into Smart Transport Systems (STS) offers a transformative approach to enhancing security and mitigating emerging cyber threats in highly connected environments. By establishing a security framework that continuously verifies every access request, regardless of the source, ZTA strengthens the resilience of transport networks against evolving risks. The research highlights the critical role of Zero Trust in addressing the increasing complexities of managing data flows, authentication, and access control in smart transport infrastructure, ensuring that both user and system data are safeguarded.

The findings emphasize the importance of seamless interoperability between various components of STS, such as traffic management systems, sensors, and vehicles, while maintaining robust security protocols. The implementation of ZTA in these systems fosters a security-first mindset that minimizes the attack surface and prevents unauthorized access, ultimately enhancing the overall safety and reliability of transportation services. Furthermore, the importance of continuously assessing and updating security policies within a Zero Trust framework is crucial for responding to new vulnerabilities in a rapidly evolving digital landscape.

Looking forward, future research should focus on the integration of advanced Artificial Intelligence (AI) to support real-time decision-making in STS. AI's ability to analyze vast amounts of data quickly and accurately will play a pivotal role in predicting security threats and improving system responsiveness. Additionally, as user privacy concerns grow in parallel with the expansion of smart technologies, further research into enhancing user privacy within ZTA frameworks is essential. This could involve developing privacy-preserving techniques that allow for secure data sharing without compromising individual privacy rights, ensuring that ZTA not only fortifies security but also promotes public trust in these technologies.

In summary, integrating ZTA into Smart Transport Systems represents a significant leap toward achieving secure, efficient, and future-proof transportation infrastructure. By continuing to advance research in AI integration and privacy enhancement, stakeholders can optimize the security capabilities of STS while maintaining the balance between innovation and user protection.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abdi, L., & Meddeb, A. (2018). Driver information system: a combination of augmented reality, deep learning and vehicular Ad-hoc networks. *Multimedia Tools and Applications*, *77*, 14673-14703.

[2] Abou Elassad, Z. E., Mousannif, H., Al Moatassime, H., & Karkouch, A. (2020). The application of machine learning techniques for driving behavior analysis: A conceptual framework and a systematic literature review. *Engineering Applications of Artificial Intelligence*, *87*, 103312.

[3] AbuAli, N., & Abou-Zeid, H. (2016). Driver behavior modeling: Developments and future directions. *International journal of vehicular technology*, *2016*(1), 6952791.

[4] Abughalieh, K. M., & Alawneh, S. G. (2020). Predicting pedestrian intention to cross the road. *IEEE Access*, *8*, 72558-72569.

[5] Aksjonov, A., & Kyrki, V. (2021, September). Rule-based decision-making system for autonomous vehicles at intersections with mixed traffic environment. In *2021 IEEE International Intelligent Transportation Systems Conference (ITSC)* (pp. 660-666). IEEE.

[6] Alizadeh, T., & Irajifar, L. (2018). Gold Coast smart city strategy: Informed by local planning priorities and international smart city best practices. *International Journal of Knowledge-Based Development*, *9*(2), 153-173.

[7] Alsrehin, N. O., Klaib, A. F., & Magableh, A. (2019). Intelligent transportation and control systems using data mining and machine learning techniques: A comprehensive study. *IEEE Access*, *7*, 49830-49857.

[8] Alzubaidi, A., & Kalita, J. (2016). Authentication of smartphone users using behavioral biometrics. *IEEE Communications Surveys & Tutorials*, *18*(3), 1998-2026.

[9] Amado, H., Ferreira, S., Tavares, J. P., Ribeiro, P., & Freitas, E. (2020). Pedestrian–vehicle interaction at unsignalized crosswalks: a systematic review. *Sustainability*, *12*(7), 2805.

[10] Araújo, S. O., Peres, R. S., Barata, J., Lidon, F., & Ramalho, J. C. (2021). Characterising the agriculture 4.0 landscape—emerging trends, challenges and opportunities. Agronomy, 11(4), 667.

[11] Arvin, R., Kamrani, M., & Khattak, A. J. (2019). How instantaneous driving behavior contributes to crashes at intersections: Extracting useful information from connected vehicle message data. Accident Analysis & Prevention, 127, 118-133.

[12] Asaithambi, G., Kanagaraj, V., & Toledo, T. (2016). Driving behaviors: Models and challenges for non-lane based mixed traffic. Transportation in Developing Economies, 2, 1-16.

[13] Austin-Gabriel, B., Hussain, N. Y., Ige, A. B., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Advancing zero trust architecture with AI and data science for enterprise cybersecurity frameworks. Open Access Research Journal of Engineering and Technology, 1(1), 47–55. https://doi.org/10.53022/oarjet.2021.1.1.0107

[14] Azadani, M. N., & Boukerche, A. (2021). Driving behavior analysis guidelines for intelligent transportation systems. IEEE transactions on intelligent transportation systems, 23(7), 6027-6045.

[15] Baheti, B., Gajre, S., & Talbar, S. (2018). Detection of distracted driver using convolutional neural network. In Proceedings of the IEEE conference on computer vision and pattern recognition workshops (pp. 1032-1038).

[16] Barlow, M., & Levy-Bencheton, C. (2018). Smart cities, smart future: Showcasing tomorrow. John Wiley & Sons.

[17] Bibri, S. E., & Bibri, S. E. (2020). The eco–city paradigm of sustainable urbanism in the era of big data revolution: A comprehensive state–of–the–art literature review. Advances in the Leading Paradigms of Urbanism and their Amalgamation: Compact Cities, Eco–Cities, and Data–Driven Smart Cities, 71-101.

[18] Bobbert, Y., & Scheerder, J. (2020). Zero trust validation: from practical approaches to theory. Sci. J. Res. Rev, 2(5), 830-848.

[19] Camara, F., Bellotto, N., Cosar, S., Weber, F., Nathanael, D., Althoff, M., ... & Fox, C. (2020). Pedestrian models for autonomous driving part ii: high-level models of human behavior. IEEE Transactions on Intelligent Transportation Systems, 22(9), 5453-5472.

[20] Cascio, W. F., & Montealegre, R. (2016). How technology is changing work and organizations. Annual review of organizational psychology and organizational behavior, 3(1), 349-375.

[21] Cello, M., Degano, C., Marchese, M., & Podda, F. (2016). Smart transportation systems (STSs) in critical conditions. In Smart Cities and Homes (pp. 291-322). Morgan Kaufmann.

[22] Chen, D., Wawrzynski, P., & Lv, Z. (2021). Cyber security in smart cities: a review of deep learning-based applications and case studies. Sustainable Cities and Society, 66, 102655.

[23] De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. Government Information Quarterly, 34(1), 1-7.

[24] de la Torre, R., Corlu, C. G., Faulin, J., Onggo, B. S., & Juan, A. A. (2021). Simulation, optimization, and machine learning in sustainable transportation systems: models and applications. *Sustainability*, *13*(3), 1551.

[25] Docherty, I., Marsden, G., & Anable, J. (2018). The governance of smart mobility. *Transportation Research Part A: Policy and Practice*, *115*, 114-125.

[26] Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., ... & Upadhyay, N. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International journal of information management*, *55*, 102211.

[27] Eom, M., & Kim, B. I. (2020). The traffic signal control problem for intersections: a review. *European transport research review*, *12*, 1-20.

[28] Essa, M. (2020). *Real-time safety and mobility optimization of traffic signals in a connected-vehicle environment* (Doctoral dissertation, University of British Columbia).

[29] Fu, C., & Liu, H. (2020). Investigating influence factors of traffic violations at signalized intersections using data gathered from traffic enforcement camera. *PLoS one*, *15*(3), e0229653.

[30] Galterio, M. G., Shavit, S. A., & Hayajneh, T. (2018). A review of facial biometrics security for smart devices. *Computers*, *7*(3), 37.

[31] Ghanipoor Machiani, S. (2015). Modeling Driver Behavior at Signalized Intersections: Decision Dynamics, Human Learning, and Safety Measures of Real-time Control Systems.

[32] Guo, Q., Li, L., & Ban, X. J. (2019). Urban traffic signal control with connected and automated vehicles: A survey. *Transportation research part C: emerging technologies*, *101*, 313-334.

[33] Hamdar, S. H., Qin, L., & Talebpour, A. (2016). Weather and road geometry impact on longitudinal driving behavior: Exploratory analysis using an empirically supported acceleration modeling framework. *Transportation research part C: emerging technologies*, *67*, 193-213.

[34] Hara, K., Kataoka, H., Inaba, M., Narioka, K., Hotta, R., & Satoh, Y. (2021). Predicting appearance of vehicles from blind spots based on pedestrian behaviors at crossroads. *IEEE transactions on intelligent transportation systems*, *23*(8), 11917-11929.

[35] Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726.

[36] Iivari, N., Sharma, S., & Ventä-Olkkonen, L. (2020). Digital transformation of everyday life–How COVID-19 pandemic transformed the basic education of the young generation and why information management research should care?. *International journal of information management*, *55*, 102183.

[37] Jiang, Q., Huang, H., Zhao, W., Baig, F., Lee, J., & Li, P. (2021). Intention of risk-taking behavior at unsignalized intersections under the connected vehicle environment. *IEEE Access*, *9*, 50624-50638.

[38] Katrakazas, C., Quddus, M., Chen, W. H., & Deka, L. (2015). Real-time motion planning methods for autonomous on-road driving: State-of-the-art and future research directions. *Transportation Research Part C: Emerging Technologies*, *60*, 416-442.

[39] Kenzie, F. (2021). Cyber-Attack Resilience in Cloud Computing: Strategies for Device and Technology Protection.

[40] Kolekar, S., Gite, S., Pradhan, B., & Kotecha, K. (2021). Behavior prediction of traffic actors for intelligent vehicle using artificial intelligence techniques: A review. *IEEE Access*, *9*, 135034-135058.

[41] Konidala, S., & Manda, J. (2020). How to implement a Zero Trust architecture for your organization using IAM. *Distributed Learning and Broad Applications in Scientific Research*, *6*, 1083-1102.

[42] Kortjan, N., & Von Solms, R. (2014). A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal*, *52*(1), 29-41.

[43] Koźlak, A. (2020). The relationship between the concepts of sharing economy and smart cities: the case of shared mobility and smart transport. *International Journal of Sustainable Society*, *12*(2), 152-184.

[44] Lee, M., Yun, J. J., Pyka, A., Won, D., Kodama, F., Schiuma, G., ... & Zhao, X. (2018). How to respond to the fourth industrial revolution, or the second information technology revolution? Dynamic new combinations between technology, market, and society through open innovation. *Journal of Open Innovation: Technology, Market, and Complexity*, *4*(3), 21.

[45] Legner, C., Eymann, T., Hess, T., Matt, C., Böhmann, T., Drews, P., ... & Ahlemann, F. (2017). Digitalization: opportunity and challenge for the business and information systems engineering community. *Business & information systems engineering*, *59*, 301-308.

[46] Li, G., Li, S., Li, S., Qin, Y., Cao, D., Qu, X., & Cheng, B. (2020). Deep reinforcement learning enabled decision-making for autonomous driving at intersections. *Automotive Innovation*, *3*, 374-385.

[47] Li, Z., Elefteriadou, L., & Ranka, S. (2014). Signal control optimization for automated vehicles at isolated signalized intersections. *Transportation Research Part C: Emerging Technologies*, *49*, 1-18.

[48] Lim, H. S. M., & Taeihagh, A. (2018). Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications. *Energies*, *11*(5), 1062.

[49] Magyari, Z., Koren, C., Kieć, M., & Borsos, A. (2021). Sight distances at unsignalized intersections: A comparison of guidelines and requirements for human drivers and autonomous vehicles. *Archives of transport*, *59*(3), 7-19.

[50] Maldonado Silveira Alonso Munhoz, P. A., da Costa Dias, F., Kowal Chinelli, C., Azevedo Guedes, A. L., Neves dos Santos, J. A., da Silveira e Silva, W., & Pereira Soares, C. A. (2020). Smart mobility: The main drivers for increasing the intelligence of urban mobility. *Sustainability*, *12*(24), 10675.

[51] Manda, J. K. (2020). Cloud Security Best Practices for Telecom Providers: Developing comprehensive cloud security frameworks and best practices for telecom service delivery and operations, drawing on your cloud security expertise. *Available at SSRN 5003526*.

[52] Martin, W. J. (2017). *The global information society*. Routledge.

[53] Mehar, S., Zeadally, S., Remy, G., & Senouci, S. M. (2014). Sustainable transportation management system for a fleet of electric vehicles. *IEEE transactions on intelligent transportation systems*, *16*(3), 1401-1414.

[54] Mena-Yedra, R. (2020). An adaptive, fault-tolerant system for road network traffic prediction using machine learning.

[55] Mosco, V. (2017). *Becoming digital: Toward a post-internet society*. Emerald Publishing Limited.

[56] Mozaffari, S., Al-Jarrah, O. Y., Dianati, M., Jennings, P., & Mouzakitis, A. (2020). Deep learning-based vehicle behavior prediction for autonomous driving applications: A review. *IEEE Transactions on Intelligent Transportation Systems*, *23*(1), 33-47.

[57] Muhirwe, J., & White, N. (2016). Cybersecurity Awareness And Practice Of Next Generation Corporate Technology Users. *Issues in Information Systems*, *17*(2).

[58] Mukherjee, D., & Mitra, S. (2019). A comparative study of safe and unsafe signalized intersections from the view point of pedestrian behavior and perception. *Accident Analysis & Prevention*, *132*, 105218.

[59] Muresan, M. (2021). Deep Reinforcement Learning Models for Real-Time Traffic Signal Optimization with Big Traffic Data.

[60] Nace, L. (2020, September). Securing Trajectory based Operations through a Zero Trust Framework in the NAS. In *2020 Integrated Communications Navigation and Surveillance Conference (ICNS)* (pp. 1B1-1). IEEE.

[61] National Academies of Sciences, Policy, Global Affairs, Technology for Sustainability Program, Committee on Pathways to Urban Sustainability, & Opportunities. (2016). Pathways to urban sustainability: challenges and opportunities for the United States.

[62] Neal, T. J., & Woodard, D. L. (2016). Surveying biometric authentication for mobile device security. *Journal of Pattern Recognition Research*, *1*(74-110), 4.

[63] Ni, D. (2020). *Signalized Intersections*. Cham, Swizerland: Springer International Publishing.

[64] Nikitas, A., Michalakopoulou, K., Njoya, E. T., & Karampatzakis, D. (2020). Artificial intelligence, transport and the smart city: Definitions and dimensions of a new mobility era. *Sustainability*, *12*(7), 2789.

[65] Olayode, I. O., Tartibu, L. K., Okwu, M. O., & Uchechi, D. U. (2020). Intelligent transportation systems, un-signalized road intersections and traffic congestion in Johannesburg: A systematic review. *Procedia CIRP*, *91*, 844-850.

[66] Pace, M. (2021). *Zero Trust networks with Istio* (Doctoral dissertation, Politecnico di Torino).

[67] Paschek, F. (2017). *Smarter cities: socio-technical innovation towards sustainable urban transport futures-the case of re-establishing utility cycling as a mainstream mode in London* (Doctoral dissertation, University of Greenwich).

[68] Pawar, D. S., & Patil, G. R. (2017). Minor-street vehicle dilemma while maneuvering at unsignalized intersections. *Journal of Transportation Engineering, Part A: Systems*, *143*(8), 04017039.

[69] Peng, H., Wang, H., Du, B., Bhuiyan, M. Z. A., Ma, H., Liu, J., ... & Philip, S. Y. (2020). Spatial temporal incidence dynamic graph neural networks for traffic flow forecasting. *Information Sciences*, *521*, 277-290.

[70] Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of scientific research and management*, *9*(12), 669-710.

[71] Petraki, V., Ziakopoulos, A., & Yannis, G. (2020). Combined impact of road and traffic characteristic on driver behavior using smartphone sensor data. *Accident Analysis & Prevention*, *144*, 105657.

[72] Porter, L., Stone, J., Legacy, C., Curtis, C., Harris, J., Fishman, E., ... & Stilgoe, J. (2018). The autonomous vehicle Revolution: Implications for planning/The driverless city?/autonomous vehicles–a planner's response/autonomous vehicles: Opportunities, challenges and the need for government action/three signs autonomous vehicles will not lead to less car ownership and less car use in car dependent cities–a case study of Sydney, Australia/planning for autonomous vehicles? Questions of purpose, place and pace/ensuring good governance: The role of planners in the development of autonomous vehicles .... *Planning Theory & Practice*, *19*(5), 753-778.

[73] Rodrigues, M., McGordon, A., Gest, G., & Marco, J. (2018). Autonomous navigation in interaction-based environments—A case of non-signalized roundabouts. *IEEE Transactions on Intelligent Vehicles*, *3*(4), 425-438.

[74] Rui, Z., & Yan, Z. (2018). A survey on biometric authentication: Toward secure and privacy-preserving identification. *IEEE access*, *7*, 5994-6009.

[75] Schmidt, E., & Cohen, J. (2015). The new digital age: Reshaping the future of people, nations and business.

[76] Schwertner, K. (2017). Digital transformation of business. *Trakia Journal of Sciences*, *15*(1), 388-393.

[77] Sendin, A., Matanza, J., & Ferrús, R. (2021). *Smart Grid Telecommunications: Fundamentals and Technologies in the 5G Era*. John Wiley & Sons.

[78] Sharma, H. (2021). Behavioral Analytics and Zero Trust. *International Journal of Computer Engineering and Technology*, *12*(1), 63-84.

[79] Shirazi, M. S., & Morris, B. T. (2016). Looking at intersections: a survey of intersection monitoring, behavior and safety analysis of recent studies. *IEEE Transactions on Intelligent Transportation Systems*, *18*(1), 4-24.

[80] Silasai, O., & Khowfa, W. (2020). The study on using biometric authentication on mobile device. *NU Int. J. Sci*, *17*, 90-110.

[81] Singh, H., & Kathuria, A. (2021). Analyzing driver behavior under naturalistic driving conditions: A review. *Accident Analysis & Prevention*, *150*, 105908.

[82] Soomro, K., Bhutta, M. N. M., Khan, Z., & Tahir, M. A. (2019). Smart city big data analytics: An advanced review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *9*(5), e1319.

[83] Sridhar, S., Gadgil, R., & Dhingra, C. (2020). *Paving the Way for Better Governance in Urban Transport*. Springer Singapore.

[84] Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information & Computer Security*, *25*(5), 494-534.

[85] Sufian, A. T., Abdullah, B. M., Ateeq, M., Wah, R., & Clements, D. (2021). Six-gear roadmap towards the smart factory. *Applied Sciences*, *11*(8), 3568.

[86] Sun, D., & Elefteriadou, L. (2014). A driver behavior-based lane-changing model for urban arterial streets. *Transportation science*, *48*(2), 184-205.

[87] Sweeney, C. (2021). *A Zero-Knowledge Multi-Factor Authentication Framework for Actualizing the Federal Zero-Trust Enterprise* (Master's thesis, Utica College).

[88] Tawari, A., Mallela, P., & Martin, S. (2018, November). Learning to attend to salient targets in driving videos using fully convolutional RNN. In *2018 21st International Conference on Intelligent Transportation Systems (ITSC)* (pp. 3225-3232). IEEE.

[89] Tian, R., Li, N., Kolmanovsky, I., Yildiz, Y., & Girard, A. R. (2020). Game-theoretic modeling of traffic in unsignalized intersection network for autonomous vehicle control verification and validation. *IEEE Transactions on Intelligent Transportation Systems*, *23*(3), 2211-2226.

[90] Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 102387.

[91] Van Deursen, A. J., & Van Dijk, J. A. (2014). *Digital skills: Unlocking the information society*. Springer.

[92] Vanolo, A. (2014). Smartmentality: The smart city as disciplinary strategy. *Urban studies*, *51*(5), 883-898.

[93] Vemori, V. (2020). Towards Safe and Equitable Autonomous Mobility: A Multi-Layered Framework Integrating Advanced Safety Protocols and XAI for Transparent Decision-Making in Self-Driving Vehicles. *Journal of Science & Technology*, *1*(1), 130-161.

[94] Wang, C., Wang, Y., Chen, Y., Liu, H., & Liu, J. (2020). User authentication on mobile devices: Approaches, threats and trends. *Computer Networks*, *170*, 107118.

[95] White, J. (2016). Cyber Threats and Cyber Security: National Security Issues, Policy and Strategies. *Global Security Studies*, *7*(4).

[96] William, S. R. (2021). Zero Trust Philosophy Versus Architecture.

[97] Wylde, A. (2021, June). Zero trust: Never trust, always verify. In *2021 international conference on cyber situational awareness, data analytics and assessment (cybersa)* (pp. 1-4). IEEE.

[98] Ye, F., Hao, P., Qi, X., Wu, G., Boriboonsomsin, K., & Barth, M. J. (2018). Prediction-based eco-approach and departure at signalized intersections with speed forecasting on preceding vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *20*(4), 1378-1389.

[99] Yuan, T., da Rocha Neto, W. B., Rothenberg, C., Obraczka, K., Barakat, C., & Turletti, T. (2019). Harnessing machine learning for next-generation intelligent transportation systems: a survey. *Proceedings of the computational intelligence, communication systems and networks (CICSyN)*.

[100] Zhang, C., Li, R., Kim, W., Yoon, D., & Patras, P. (2020). Driver behavior recognition via interwoven deep convolutional neural nets with multi-stream inputs. *Ieee Access*, *8*, 191138-191151.

[101] Zhang, H., & Fu, R. (2020). A hybrid approach for turning intention prediction based on time series forecasting and deep learning. *Sensors*, *20*(17), 4887.

[102] Zhang, J. (2020). *An investigation of smart transportation system (STS) data integration within Chinese cities: A socio-technical system perspective* (Doctoral dissertation, University of Sheffield).

[103] Zhang, Y., Yan, X., Wu, J., & Duan, K. (2020). Effect of warning system on interactive driving behavior at unsignalized intersection under fog conditions: a study based on multiuser driving simulation. *Journal of advanced transportation*, *2020*(1), 8871875.