Digital Transformation for Secure and Sustainable Systems: Advances in Privacy, Authentication, Intelligent Construction, and Connected Mobility

Madhab Chandra Jena, Om Krishna Jena

GIFT Autonomous, Bhubaneswar, Odisha, India, Email: madhab_jena@rediffmail.com
CIPET, Bhubaneswar, Odisha, India, Email: omkrishnajena2007@gmail.com

Corresponding Author: Madhab Chandra Jena, Email: madhab_jena@rediffmail.com

How to Cite this Article:

Jena, M. C. & Jena, O. K. (2026). Digital Transformation for Secure and Sustainable Systems: Advances in Privacy, Authentication, Intelligent Construction, and Connected Mobility. International Journal of Creative and Open Research in Engineering and Management, <i>02</i>(8), 1-9. https://doi.org/10.55041/ijcope.v2i8.265

https://doi.org/10.55041/ijcope.v2i8.265

Abstract

Digital transformation is increasingly reshaping infrastructure systems by integrating connected technologies, intelligent decision-making, automated processes, and sustainable resource management. However, the rapid expansion of digital infrastructure has also introduced challenges related to cybersecurity, privacy, interoperability, scalability, environmental impact, and operational resilience. This study presents a systematic review of digital technologies for sustainable and secure infrastructure, with particular emphasis on connected vehicles, privacy-preserving technologies, and intelligent construction. The review examines two complementary domains: secure connected transportation and digitally enabled sustainable construction. In the transportation domain, attention is given to authentication, privacy protection, pseudonym management, Sybil resistance, accountability, zero-trust architectures, decentralized trust, and infrastructure-assisted security. In the construction domain, the review considers digital inspection, three-dimensional concrete printing, sustainable construction materials, and digitally supported supply-chain resilience. The analysis identifies common challenges across both domains, including the need for trustworthy data exchange, interoperability, scalable architectures, efficient resource utilization, and balanced protection of privacy and accountability. The findings indicate that digitalization should not be evaluated solely in terms of technological performance but through an integrated framework incorporating security, sustainability, resilience, economic feasibility, and lifecycle performance. The study further identifies opportunities for integrating artificial intelligence, edge computing, digital twins, privacy-preserving analytics, and energy-efficient cybersecurity into future infrastructure systems. The review provides a conceptual foundation for developing infrastructure that is not only intelligent and connected but also secure, sustainable, adaptive, and resilient.

Keywords: Digital transformation; Sustainable infrastructure; Secure infrastructure; Connected vehicles; VANETs; Privacy preservation; Cybersecurity; Intelligent construction; Digital inspection; 3D-printed concrete; Supply-chain resilience; Zero-trust security; Blockchain; Artificial intelligence; Digital twins.

1. Introduction

1.1 Background

Digital transformation has become an important driver of change in infrastructure development, particularly as physical systems increasingly depend on connected devices, intelligent communication networks, data-driven decision-making, and automated management processes. Infrastructure is no longer limited to physical assets such as roads, buildings, transportation networks, and construction facilities. Instead, modern infrastructure increasingly combines physical assets with digital platforms, sensing technologies, communication networks, computational intelligence, and cybersecurity mechanisms. This transition has created new opportunities for improving efficiency, sustainability, safety, quality, and operational resilience. At the same time, it has introduced new risks related to privacy, authentication, cyberattacks, data integrity, and dependence on digital supply chains.

The transformation is visible in both connected transportation and construction environments. In connected transportation, Vehicular Ad Hoc Networks (VANETs) enable vehicles and roadside infrastructure to exchange information to support traffic management, safety applications, mobility services, and intelligent transportation systems. However, the open and highly dynamic nature of vehicular communication creates significant security and privacy challenges. Authentication mechanisms must distinguish legitimate vehicles from malicious participants while protecting users from unnecessary disclosure of identity and location information. Research has consequently examined pseudonym-based authentication, privacy preservation, Sybil resistance, accountability, and decentralized security mechanisms [5–8].

At the same time, digitalization is changing the construction sector. Digital inspection protocols can improve quality-control processes in high-rise construction by supporting systematic data collection, monitoring, and verification [1]. Three-dimensional concrete printing has also emerged as a potentially important technology for modular and sustainable construction because it can alter conventional construction processes, reduce material waste, and improve manufacturing flexibility [2]. Similarly, the use of recycled aggregates and supplementary cementitious materials provides opportunities to improve the environmental performance of concrete while maintaining appropriate structural and durability characteristics [3]. Construction organizations are also increasingly required to manage supply-chain disruptions and material-price volatility through more resilient and digitally supported management frameworks [4].

These developments indicate that digital infrastructure should be understood as a multidisciplinary system in which technological performance, cybersecurity, sustainability, and operational resilience are interconnected. A digitally advanced system cannot be considered fully effective if it improves efficiency while exposing sensitive information, increasing cyber risk, or creating unsustainable resource requirements. Conversely, a sustainable infrastructure system may remain vulnerable if its digital components lack appropriate authentication, privacy, and security mechanisms.

1.2 Digital Transformation of Infrastructure

Digital infrastructure integrates physical assets with information and communication technologies to enable real-time monitoring, automated decision-making, remote management, and data-driven optimization. In connected mobility, vehicles, roadside units, communication networks, and trusted authorities form an ecosystem in which information must be exchanged rapidly and securely. Privacy-preserving authentication is therefore a central requirement because vehicles need to demonstrate legitimacy without continuously revealing their permanent identities [9–12].

Several studies have proposed authentication mechanisms based on pseudonyms, location information, and cryptographic techniques. These approaches attempt to balance authentication efficiency with privacy protection. Pseudonym-based mechanisms are particularly important because they allow a vehicle to communicate under temporary identifiers while reducing the possibility of continuously linking communication records to a specific user. However, frequent pseudonym changes also introduce management and accountability challenges. A secure infrastructure therefore requires mechanisms that can protect anonymity during normal operation while allowing legitimate authorities to establish accountability under predefined conditions [9,10].

The development of connected infrastructure has also increased interest in decentralized technologies. Blockchain-based approaches have been investigated for authentication, trust management, and secure information exchange in VANET environments [17,19,22,23]. These approaches seek to reduce dependence on a single centralized authority and provide tamper-resistant records of relevant transactions or security events. Nevertheless, blockchain integration can introduce additional computational, communication, storage, and governance requirements. Consequently, decentralization should not automatically be regarded as a solution to every security problem.

In construction, digital transformation follows a different but complementary pathway. Digital inspection protocols can support more systematic quality-control management by improving the documentation and monitoring of construction activities [1]. Three-dimensional printing introduces digital control directly into the physical production process, linking computational design with automated material deposition [2]. Sustainable concrete technologies similarly require digital and engineering decision-making to determine appropriate combinations of recycled aggregates and supplementary cementitious materials [3]. Digital approaches can also strengthen supply-chain planning by helping organizations identify disruptions, evaluate material-price risks, and develop alternative procurement strategies [4].

Thus, digital transformation across infrastructure can be viewed through three related dimensions: intelligent operation, secure information management, and sustainable resource utilization. The first dimension concerns the ability of digital systems to monitor and optimize infrastructure. The second concerns protection against unauthorized access, privacy violations, and cyberattacks. The third concerns the reduction of resource consumption, waste, environmental impacts, and operational vulnerability.

1.3 Security and Privacy as Infrastructure Requirements

Security and privacy are particularly important when infrastructure systems collect information continuously. Connected vehicles may generate information related to location, movement, communication patterns, and service usage. If these data are inadequately protected, attackers may exploit them for tracking, impersonation, manipulation, or disruption. Consequently, authentication mechanisms must provide more than simple identity verification. They should also address confidentiality, integrity, anonymity, unlinkability, accountability, and resistance to malicious participants.

The literature demonstrates increasing attention to privacy-preserving authentication in VANETs. Two-level authentication protocols, location-based conditional privacy-preserving schemes, pseudonym renewal mechanisms, and roadside-unit-based authentication have all been investigated [10–13,18]. These approaches reflect an important design tension: stronger privacy may make accountability more difficult, while stronger traceability may increase the risk of surveillance.

Sybil attacks represent another important challenge. In a Sybil attack, a malicious participant creates multiple false identities to influence network decisions or communication processes. The development of Sybil-free authentication mechanisms therefore represents an important step toward trustworthy connected mobility [5]. Such mechanisms need to ensure that multiple identities cannot be generated or exploited by the same unauthorized participant while preserving legitimate privacy requirements.

The emergence of vehicle-rental applications adds another layer of complexity. Vehicle-rental systems require mechanisms that can authenticate users and vehicles while preserving privacy and establishing accountability when misuse occurs. Research on privacy-preserving vehicle renting has examined these requirements in VANET environments [6,7]. The incorporation of zero-trust principles further emphasizes the need to avoid implicit trust and continuously verify users, devices, and interactions [6].

Cybersecurity concerns are not limited to vehicular systems. Cloud environments supporting infrastructure applications can also contain covert communication channels and other attack surfaces. Research on multi-covert-channel attacks demonstrates how attackers may exploit shared or cloud-based resources to conceal malicious communication [8]. This highlights the importance of considering the complete digital ecosystem rather than securing only the communication layer.

1.4 Sustainability and Intelligent Construction

The sustainability dimension of digital infrastructure is particularly relevant to construction because buildings and infrastructure projects consume substantial quantities of materials, energy, labor, and financial resources. Digital technologies can support sustainability by improving planning, reducing waste, monitoring quality, and enabling alternative construction techniques.

Digital inspection protocols represent one such application. Conventional inspection processes may depend heavily on manual documentation and fragmented information flows. Digital inspection can provide a more systematic approach to recording construction conditions and verifying quality requirements [1]. Such systems can potentially improve traceability and reduce errors associated with incomplete or inconsistent inspection records.

Three-dimensional concrete printing represents a more direct integration between digital technology and physical construction. Digital models can be translated into automated construction operations, creating opportunities for greater geometric flexibility and potentially reduced material waste [2]. However, the sustainability performance of 3D-printed concrete depends on material composition, printing efficiency, structural requirements, energy consumption, and lifecycle considerations. Digital fabrication should therefore be evaluated not only according to its technological novelty but also according to its environmental and economic performance.

Material innovation provides another pathway toward sustainable infrastructure. The incorporation of recycled aggregates and supplementary cementitious materials can reduce dependence on conventional raw materials and contribute to improved resource efficiency [3]. Nevertheless, the use of alternative materials requires careful evaluation of structural performance and durability. Digital monitoring and data-driven material optimization could potentially strengthen this process by enabling more systematic evaluation of material combinations.

Supply-chain resilience is equally important. Disruptions in material availability and fluctuations in material prices can significantly affect construction schedules, project costs, and sustainability objectives. Frameworks addressing supply-chain disruption and material-price volatility therefore have an important role in sustainable construction management [4]. Digital tools can strengthen these frameworks by improving forecasting, supplier monitoring, inventory management, and scenario analysis.

1.5 Rationale for an Integrated Review

The existing literature demonstrates considerable progress in individual areas of digital infrastructure, but research is often organized around specific technological domains. VANET studies tend to focus on authentication, privacy, trust, blockchain, and cyberattack resistance [5–23], whereas construction studies generally emphasize digital inspection, automated fabrication, sustainable materials, and supply-chain resilience [1–4]. This separation can obscure the broader relationship between digitalization, security, and sustainability.

An integrated perspective is therefore valuable because the infrastructure of the future will increasingly depend on interconnected digital and physical systems. Connected transportation systems will require secure communication and privacy protection, while digitally enabled construction systems will require trustworthy data, resilient supply chains, and sustainable production methods. Both domains ultimately depend on the reliability of digital information and the ability of organizations to manage technological risks.

The present review consequently examines digital technologies through two complementary perspectives: secure connected infrastructure and sustainable intelligent construction. The objective is not to assume that VANET technologies can be directly transferred to construction or that construction technologies can directly solve vehicle-network security problems. Instead, the review identifies common principles, including trusted digital interaction, data protection, resilience, automation, resource efficiency, and lifecycle-oriented decision-making.

1.6 Objectives and Scope of the Review

The main objective of this review is to synthesize research on digital technologies that contribute to secure, sustainable, and intelligent infrastructure. The review focuses on four principal objectives.

First, it examines the development of privacy-preserving authentication and security mechanisms for connected vehicles, including pseudonym systems, Sybil-resistant authentication, zero-trust mechanisms, and blockchain-based approaches [5–23].

Second, it evaluates the role of digital technologies in sustainable construction, particularly digital inspection, 3D-printed concrete, sustainable concrete materials, and supply-chain resilience [1–4].

Third, it identifies common challenges affecting digital infrastructure, including privacy protection, accountability, cybersecurity, scalability, interoperability, resource consumption, implementation complexity, and organizational adoption.

Finally, it develops an integrated research perspective in which security, sustainability, and digital intelligence are treated as complementary requirements rather than independent objectives.

2. Digital Technologies for Secure Connected Infrastructure

2.1 Connected Vehicles and VANET Security

Connected vehicles have become an important component of intelligent transportation infrastructure because they enable vehicles, roadside units, and infrastructure platforms to exchange information in real time. Vehicular Ad Hoc Networks (VANETs) support applications such as collision avoidance, traffic coordination, route optimization, emergency notifications, and intelligent mobility services. However, the highly dynamic topology of VANETs, large number of participating vehicles, wireless communication environment, and limited tolerance for communication delays create substantial security challenges. Unlike conventional communication networks, vehicular systems must often authenticate participants rapidly while maintaining privacy and ensuring that malicious vehicles cannot manipulate network operations.

Authentication is therefore a fundamental security requirement in connected transportation. A vehicle must be able to demonstrate that it is an authorized participant without unnecessarily revealing its permanent identity. At the same time, infrastructure operators need mechanisms for identifying or tracing malicious users when serious security violations occur. This creates a fundamental tension between anonymity and accountability. Privacy-preserving authentication schemes attempt to address this problem by using temporary identities, pseudonyms, cryptographic credentials, and conditional traceability [9–12].

The importance of this issue is particularly evident in safety-critical vehicular applications. False messages regarding traffic conditions, vehicle positions, accidents, or road hazards can result in inappropriate decisions and potentially dangerous situations. Consequently, authentication cannot be considered independently from message integrity and trust management. A secure VANET must establish confidence that the sender is legitimate and that transmitted information has not been manipulated.

2.2 Privacy-Preserving Authentication

Privacy preservation has become one of the major research themes in VANET security. Connected vehicles may continuously generate information concerning location, movement patterns, communication behavior, and service usage. If permanent identifiers are attached to such information, an adversary may potentially track vehicles over extended periods. Pseudonym-based authentication has therefore been proposed as a mechanism for separating authentication from persistent identification.

Location-based conditional privacy-preserving authentication is one approach that attempts to balance these competing requirements. Such mechanisms can authenticate vehicles while limiting exposure of their long-term identities [10]. Similarly, two-level pseudonymous authentication has been investigated to provide stronger privacy while maintaining the ability to authenticate legitimate vehicles [11]. These approaches demonstrate that privacy protection should be incorporated into the authentication architecture rather than treated as an additional feature after the security system has been designed.

Pseudonym renewal is another important component of privacy protection. If a vehicle continuously uses the same pseudonym, an observer may still link multiple messages to the same vehicle even without knowing its real identity. Pseudonym-changing mechanisms can reduce such linkability by allowing vehicles to periodically adopt new identifiers [9,12]. However, pseudonym changes must be carefully managed because excessive changes may increase communication and computational overhead, while poorly coordinated changes may reduce the effectiveness of authentication and accountability.

Privacy-preserving authentication has also been investigated in specific vehicular service environments. For example, vehicle-rental applications require authentication of both users and vehicles while protecting sensitive information associated with rental transactions. The privacy-preserving vehicle-rental framework proposed by Akil et al. addresses the challenge of maintaining user privacy while supporting driver accountability in VANET environments [7]. This demonstrates that privacy requirements extend beyond conventional vehicle-to-vehicle communication and become increasingly important as connected vehicles are integrated with commercial and mobility services.

2.3 Sybil Attacks and Identity Management

Sybil attacks represent a particularly serious threat to connected transportation systems because an attacker may generate or control multiple identities and use them to influence network decisions. In a vehicular environment, multiple fraudulent identities could be used to create false impressions about traffic density, vehicle positions, congestion, or consensus among network participants. Such attacks can undermine trust even when the underlying communication protocol is technically functional.

Akil et al. proposed a non-interactive privacy-preserving authentication scheme designed to provide Sybil-free authentication in VANETs [5]. The importance of this approach lies in its attempt to address both identity multiplicity and privacy. A security mechanism that simply prevents multiple identities by requiring permanent identification may reduce Sybil attacks but can simultaneously create significant privacy concerns. A more appropriate approach must prevent unauthorized identity multiplication while preserving the anonymity of legitimate participants.

Identity management is therefore a central element of secure connected infrastructure. The challenge is not simply to determine whether a message comes from an authenticated entity, but also to determine whether the same physical or logical participant is improperly represented by multiple identities. This requires carefully designed credential-generation, pseudonym-management, and revocation mechanisms.

Pseudonym systems also create an important trade-off between privacy and accountability. Strong anonymity can make it difficult to identify malicious participants, whereas extensive traceability can expose users to surveillance. Conditional privacy therefore appears to be a more practical direction in which ordinary communication remains private while authorized entities can establish accountability when predefined conditions are satisfied [9–13].

2.4 Zero-Trust Security in Connected Vehicles

Traditional network-security architectures often assume that entities operating within an authorized environment can be trusted after successful authentication. Such assumptions become increasingly problematic in highly connected vehicular environments where vehicles, users, roadside units, cloud services, and external applications continuously interact.

Zero-trust security provides an alternative approach based on the principle that authentication should not automatically imply continuous trust. Instead, access and interaction should be evaluated according to identity, context, authorization, and security conditions. Akil et al. applied a zero-trust perspective to vehicle renting in VANETs, emphasizing secure and privacy-preserving interactions between users, vehicles, and network services [6].

The zero-trust approach is particularly relevant as vehicular ecosystems become more integrated with external digital platforms. A vehicle may simultaneously interact with roadside infrastructure, cloud services, rental platforms, payment systems, and other vehicles. Each connection potentially creates an attack surface. Consequently, security mechanisms must consider not only the initial authentication event but also the legitimacy of subsequent requests and interactions.

The zero-trust perspective also complements pseudonym-based privacy mechanisms. Authentication can establish that a participant is authorized without unnecessarily exposing its permanent identity, while contextual authorization can determine whether a particular action should be permitted. This combination may provide a more flexible security architecture for future connected-mobility platforms.

2.5 Blockchain and Decentralized Trust

Blockchain technology has attracted attention as a mechanism for improving trust, authentication, and transaction integrity in distributed vehicular environments. A major motivation is the possibility of maintaining tamper-resistant records without depending entirely on a single centralized authority. Research has consequently examined blockchain-based authentication and trust-management mechanisms for VANETs [17,19,22,23].

Blockchain-based architectures can potentially support decentralized credential management, transaction verification, trust evaluation, and accountability. In a connected-vehicle environment, this could be useful when multiple organizations participate in the infrastructure and no single organization has complete control over all communication processes. A distributed ledger may provide a common record of relevant security events or transactions.

However, blockchain does not automatically solve the fundamental privacy and scalability challenges of VANETs. Vehicular networks can generate large volumes of rapidly changing data, while blockchain systems may involve communication, computation, storage, and consensus overhead. Therefore, blockchain-based solutions need to be evaluated according to latency, scalability, energy consumption, transaction throughput, and privacy protection rather than solely according to their decentralization properties.

Comprehensive studies of blockchain-based VANET architectures have highlighted the potential of distributed ledger technologies for authentication, trust management, data integrity, and decentralized coordination [19]. Other research has specifically investigated blockchain-supported privacy-preserving authentication mechanisms [17,22,23]. These studies suggest that blockchain is most useful when it addresses a clearly defined trust or coordination problem rather than being introduced simply as a general-purpose security technology.

2.6 SDN and Infrastructure-Assisted Security

Software-Defined Networking (SDN) provides another technological direction for improving the management of vehicular communication networks. By separating control functions from forwarding functions, SDN can provide greater flexibility in network configuration, monitoring, and policy enforcement. Privacy-preserving authentication based on SDN has therefore been investigated as a means of strengthening security in VANET environments [21].

The infrastructure-assisted nature of SDN can potentially help address some of the management challenges associated with highly dynamic vehicular networks. Centralized or logically centralized control can provide network-wide visibility and enable security policies to be updated according to changing conditions. However, excessive centralization can also introduce a single point of failure or a highly attractive target for attackers. Secure SDN architectures must therefore protect both the control plane and the communication infrastructure.

This issue reinforces a broader principle emerging from the literature: connected infrastructure requires a balance between centralized coordination and decentralized trust. Centralized mechanisms can improve manageability, while decentralized mechanisms can reduce dependence on a single authority. The most appropriate architecture may therefore depend on the application, network scale, latency requirements, and security objectives.

2.7 Roadside Units and Authentication Infrastructure

Roadside Units (RSUs) provide important infrastructure support for connected vehicles. They can facilitate communication between vehicles and network services, distribute security credentials, support authentication, and assist with traffic-management functions. RSU-based authentication has therefore been explored as an alternative or complementary mechanism for improving vehicular network security [18].

The positioning of RSUs within the physical transportation environment provides advantages for authentication and communication management. However, RSUs themselves must be treated as security-critical infrastructure. Compromise of an RSU could potentially affect a large number of vehicles operating within its communication range. Consequently, secure key management, credential protection, mutual authentication, intrusion detection, and secure software updates are essential.

RSU-based mechanisms also illustrate the relationship between physical and digital infrastructure. The security of a connected transportation system cannot be achieved solely through software running inside vehicles. Roadside infrastructure, communication channels, cloud services, and credential authorities must all be incorporated into the security architecture.

2.8 Authentication Efficiency and Scalability

Security mechanisms for VANETs must operate under stringent performance requirements. Vehicles can move rapidly between communication zones, resulting in frequent changes in network topology. Authentication procedures that are computationally expensive or communication-intensive may introduce delays that are unacceptable for safety-related applications.

Research on privacy-preserving authentication has consequently focused on improving computational efficiency while maintaining security guarantees [10–16]. Survey studies indicate that authentication schemes should be assessed according to several dimensions, including computational cost, communication overhead, privacy protection, scalability, resistance to attacks, and suitability for dynamic vehicular environments [14–16].

A particularly important issue is the trade-off between security strength and operational efficiency. Strong cryptographic mechanisms may provide better protection but can require greater computational resources. Similarly, frequent pseudonym changes can improve privacy but increase certificate-management requirements. Blockchain and decentralized architectures may strengthen trust but introduce additional processing and communication overhead [17,19,22,23].

Therefore, the performance of a VANET security mechanism should not be evaluated using a single metric. A comprehensive assessment should consider authentication delay, computational complexity, communication overhead, storage requirements, privacy level, attack resistance, scalability, and energy consumption.

2.9 Cloud and Covert-Channel Threats

Connected infrastructure increasingly depends on cloud and edge-computing resources. These platforms provide computational capacity for storing and processing data generated by vehicles and infrastructure. However, cloud environments also introduce additional attack surfaces.

Research on multi-covert-channel attacks demonstrates that attackers may exploit shared cloud resources to establish hidden communication channels [8]. Although this work is not specifically limited to VANETs, its implications are relevant to connected infrastructure because vehicular systems increasingly depend on cloud-based services. An attacker who compromises cloud or edge infrastructure may potentially bypass some of the security assumptions implemented at the vehicle level.

This highlights the importance of adopting an end-to-end security perspective. Vehicle authentication alone is insufficient if the cloud platform processing vehicular information is compromised. Similarly, secure cloud infrastructure cannot compensate for weak authentication mechanisms at the vehicle or roadside level. Security must therefore extend across vehicles, RSUs, communication networks, edge platforms, cloud infrastructure, and service providers.

2.10 Research Gaps in Secure Connected Infrastructure

The reviewed literature demonstrates substantial progress in VANET authentication, privacy protection, Sybil resistance, blockchain, zero-trust security, SDN, and infrastructure-assisted authentication [5–23]. Nevertheless, several research gaps remain.

First, privacy and accountability continue to represent competing requirements. Existing pseudonym and privacy-preserving schemes can reduce identity exposure, but reliable mechanisms for conditional traceability and efficient revocation remain important.

Second, many proposed solutions are evaluated primarily through simulations or theoretical security analyses. Greater emphasis is required on real-world deployments involving heterogeneous vehicles, roadside units, communication technologies, cloud platforms, and service providers.

Third, scalability remains a major concern. Future vehicular systems may involve extremely large numbers of connected vehicles and high-frequency message exchanges. Security mechanisms must therefore operate efficiently without creating excessive communication or computational overhead.

Fourth, the integration of different security technologies requires further investigation. Zero-trust architectures, blockchain, SDN, pseudonym systems, and conventional cryptographic authentication are often studied separately. More research is needed to determine how these technologies can be combined without creating excessive complexity.

Fifth, sustainability should be incorporated into security evaluation. Cryptographic processing, blockchain consensus, communication infrastructure, and large-scale data processing all consume computational and energy resources. A security mechanism that provides strong protection but imposes excessive energy or hardware requirements may not be appropriate for sustainable digital infrastructure.

Finally, security should be considered together with infrastructure resilience. Connected transportation systems must remain operational during cyberattacks, communication failures, infrastructure outages, and rapidly changing environmental conditions. Future research should therefore move from isolated authentication mechanisms toward integrated security architectures capable of maintaining privacy, trust, availability, and operational continuity.

3. Digital Technologies for Sustainable and Intelligent Construction

3.1 Digitalization of the Construction Sector

The construction sector is undergoing a gradual transformation from conventional, manually intensive processes toward digitally enabled planning, monitoring, fabrication, inspection, and supply-chain management. The integration of digital technologies can improve the coordination of construction activities, enhance quality control, reduce material waste, and support more informed decision-making. At the same time, increasing dependence on digital systems creates new requirements for data reliability, cybersecurity, interoperability, and organizational capability.

Digital transformation in construction differs from digitalization in connected vehicles because the physical processes, project structures, and operational time scales are different. Nevertheless, both domains depend on reliable data, trusted digital interactions, and effective management of distributed information. In construction, these requirements are particularly important because errors in inspection, material selection, fabrication, or supply-chain decisions can affect structural performance, project schedules, cost, and environmental outcomes.

The reviewed construction literature provides four important technological perspectives: digital inspection and quality management, 3D-printed concrete, sustainable concrete materials, and supply-chain resilience [1–4]. Together, these areas demonstrate how digital technologies can contribute to more intelligent and sustainable infrastructure development.

3.2 Digital Inspection and Quality Control

Quality control is a fundamental requirement in construction because defects or deviations introduced during construction can affect safety, durability, cost, and long-term performance. Conventional inspection practices frequently involve manual observations, paper-based records, fragmented communication, and retrospective identification of defects. These limitations can reduce the speed and consistency of quality-control activities.

Digital inspection protocols provide an opportunity to improve this process by enabling structured recording, monitoring, documentation, and verification of construction activities. Parikh examined the implementation of digital inspection protocols for enhanced quality-control management in high-rise construction [1]. The study highlights the role of digital processes in improving the systematic management of inspection information.

The importance of digital inspection extends beyond documentation. A digital inspection system can potentially create a traceable information flow between field observations, quality requirements, responsible personnel, corrective actions, and final verification. Such traceability can improve accountability and reduce the likelihood that critical information is lost between different stages of a project.

Digital inspection can also support data-driven decision-making. When inspection information is stored in a structured digital environment, project managers can identify recurring defects, compare performance across construction activities, and prioritize corrective measures. Over time, accumulated inspection data can support predictive quality-management approaches.

However, digital inspection should not be regarded simply as a replacement for paper records. Its effectiveness depends on data accuracy, interoperability, user acceptance, network availability, cybersecurity, and integration with existing project-management processes. A technically sophisticated inspection platform may provide limited value if construction personnel find it difficult to use or if the information cannot be integrated with other project systems.

3.3 Three-Dimensional Printed Concrete

Three-dimensional printing is one of the most significant emerging technologies in digitally enabled construction. Unlike conventional construction methods, 3D concrete printing can translate a digital design directly into an automated fabrication process. This creates opportunities for geometric customization, automation, reduced dependence on formwork, and potentially more efficient material utilization.

Parikh investigated the feasibility and efficiency of 3D-printed concrete technology in sustainable modular construction [2]. The study reflects the growing interest in combining digital fabrication with modular construction principles. Digital production can provide greater control over construction geometry and potentially improve repeatability in standardized building components.

From a sustainability perspective, 3D printing may provide several potential benefits. Automated deposition can allow material to be placed primarily where it is required, potentially reducing unnecessary material use. The elimination or reduction of conventional formwork may also decrease associated material consumption and construction waste. Furthermore, digital fabrication can support modular production, which may improve manufacturing efficiency and reduce construction-site activities.

Nevertheless, the sustainability performance of 3D-printed concrete is not automatically superior to conventional construction. Environmental performance depends on the cement content of the printable material, printing energy, transportation requirements, curing conditions, equipment utilization, and end-of-life considerations. Consequently, 3D printing should be assessed through a lifecycle perspective rather than by considering only the efficiency of the printing process.

The technology also introduces new quality-control requirements. Printing parameters such as extrusion rate, layer height, deposition speed, interlayer bonding, material rheology, and curing conditions can influence final structural performance. Digital monitoring systems can therefore play an important role in ensuring that printed components conform to design and performance requirements.

3.4 Sustainable Concrete Materials

Concrete production is closely associated with resource consumption and environmental impacts. The use of alternative materials is therefore an important component of sustainable construction. Recycled aggregates and supplementary cementitious materials have attracted attention because they can reduce reliance on conventional raw materials while potentially improving resource efficiency.

Parikh examined the optimization of structural and durability performance of concrete incorporating recycled aggregates and supplementary cementitious materials [3]. This work illustrates the need to balance environmental objectives with engineering requirements. Sustainable materials cannot be evaluated solely according to their ability to reduce conventional material consumption; they must also provide appropriate strength, durability, reliability, and service life.

Recycled aggregates can contribute to circular material flows by recovering construction and demolition waste for use in new concrete. However, their properties can differ from those of natural aggregates, and these differences may influence workability, strength development, water absorption, and durability. Supplementary cementitious materials can also modify concrete behavior while potentially reducing dependence on Portland cement.

Digital technologies can strengthen the optimization of sustainable concrete by supporting data collection, material characterization, predictive modelling, and quality monitoring. Data-driven approaches could allow engineers to evaluate multiple material combinations and identify formulations that balance strength, durability, cost, and environmental performance.

This suggests an important connection between material sustainability and digital intelligence. The environmental benefit of alternative materials can be increased when digital systems are used to optimize their composition and monitor their performance. In this context, digitalization acts not only as an administrative tool but also as an enabler of material innovation.

3.5 Supply-Chain Resilience and Material Volatility

Construction sustainability depends not only on material selection but also on the reliability of material supply. Disruptions caused by transportation problems, shortages, geopolitical events, market fluctuations, supplier failures, and unexpected price increases can affect construction schedules and project budgets.

Parikh proposed frameworks for mitigating supply-chain disruptions and material-price volatility in sustainable building construction [4]. The research highlights the importance of developing strategies that allow construction organizations to respond to uncertainty while maintaining sustainability objectives.

Digital technologies can support supply-chain resilience through real-time information sharing, demand forecasting, supplier monitoring, inventory optimization, and scenario analysis. Digital platforms can potentially integrate information from suppliers, contractors, logistics providers, and project managers to create a more transparent view of material availability and cost conditions.

Predictive analytics can also help organizations identify potential disruptions before they become critical. For example, historical purchasing data, market information, transportation conditions, and supplier performance indicators can be combined to estimate potential shortages or price increases. Such information can support early procurement decisions and alternative sourcing strategies.

However, increased digital connectivity also introduces cybersecurity and data-governance concerns. Supply-chain platforms may contain commercially sensitive information related to prices, suppliers, inventories, contractual arrangements, and procurement strategies. Unauthorized access or manipulation of such data could produce significant economic consequences. Consequently, secure digital infrastructure is an important prerequisite for digitally enabled construction supply chains.

3.6 Digital Technologies and Construction Sustainability

The relationship between digitalization and sustainability in construction is multidimensional. Digital technologies can contribute to sustainability by improving resource efficiency, reducing waste, increasing process accuracy, supporting predictive maintenance, and improving supply-chain coordination. However, digital technologies also require hardware, communication infrastructure, energy, data storage, and technical expertise.

Digital inspection provides one example of how information efficiency can support sustainability [1]. By identifying defects earlier and improving quality management, digital inspection can reduce rework, material waste, and unnecessary resource consumption. Similarly, 3D printing can potentially reduce material waste through controlled deposition and digital fabrication [2].

Sustainable material optimization provides another pathway. The combination of recycled aggregates and supplementary cementitious materials can contribute to resource conservation, while digital modelling and monitoring can help ensure that the resulting concrete satisfies structural and durability requirements [3].

Supply-chain digitalization can further support sustainability by reducing unnecessary inventory, improving logistics, and enabling organizations to respond more effectively to disruptions [4]. Thus, the sustainability benefits of digitalization arise not from a single technology but from the interaction between data, processes, materials, and decision-making.

3.7 Digital Security in Intelligent Construction

As construction projects become increasingly dependent on digital platforms, security becomes an important component of intelligent construction. Digital inspection records, building information, material data, supplier information, design models, and project-management data can contain valuable or sensitive information. Unauthorized modification of such information could affect project decisions and potentially compromise construction quality.

The security principles developed in connected-vehicle research provide useful conceptual insights for this environment. Authentication mechanisms can help ensure that only authorized personnel access project information. Privacy-preserving approaches can limit unnecessary exposure of sensitive information, while accountability mechanisms can establish responsibility for important digital actions [5–7].

The concept of zero trust is particularly relevant. Rather than assuming that users or devices operating within a project network are automatically trustworthy, access should be evaluated according to identity, authorization, context, and risk. This principle can be adapted to digitally connected construction environments involving contractors, consultants, suppliers, inspectors, project managers, and automated systems.

Similarly, blockchain-based approaches may provide opportunities for tamper-resistant records of selected construction transactions or quality-control events [17,19,22,23]. For example, digital records associated with material delivery, inspection approval, certification, or supply-chain transactions could potentially be maintained in a tamper-resistant environment.

However, the adoption of these technologies must be carefully justified. Construction organizations may have limited technical resources, and highly complex security systems may increase implementation costs and operational burden. Therefore, security architecture should be proportionate to the value and sensitivity of the information being protected.

3.8 Interoperability and Data Integration

One of the major challenges facing intelligent construction is interoperability. Construction projects involve multiple organizations using different software platforms, data formats, sensors, databases, and management systems. If these systems cannot exchange information effectively, the potential benefits of digitalization are reduced.

Digital inspection data should ideally connect with project-management systems, design information, scheduling platforms, quality records, and maintenance databases [1]. Similarly, 3D printing systems require integration between digital models, material specifications, printing equipment, monitoring systems, and quality-control processes [2].

Supply-chain platforms must also communicate with procurement, inventory, logistics, and financial systems [4]. Such integration requires common data structures, reliable interfaces, appropriate access controls, and organizational agreements concerning data ownership and responsibility.

Interoperability is therefore both a technical and organizational challenge. Even when appropriate technical standards exist, organizations may use incompatible workflows or restrict data sharing because of contractual, commercial, or security concerns.

3.9 Human and Organizational Factors

The effectiveness of intelligent construction technologies depends heavily on human and organizational factors. Construction personnel may resist new technologies when they perceive them as difficult to use, disruptive to established workflows, or associated with additional administrative requirements.

Digital inspection systems, for example, require inspectors and site personnel to enter information accurately and consistently [1]. Similarly, successful implementation of 3D printing requires operators, engineers, designers, and construction managers to develop new technical capabilities [2].

The adoption of sustainable materials also requires knowledge of material behavior and appropriate quality-control procedures [3]. Supply-chain digitalization requires personnel capable of interpreting forecasts, monitoring suppliers, and responding to risk information [4].

Training and organizational readiness are therefore critical. Digital transformation should not be treated solely as a technology-acquisition process. It requires changes in workflows, responsibilities, skills, governance, and performance evaluation.

3.10 Integration of Secure and Sustainable Digital Infrastructure

The evidence from the reviewed studies suggests that sustainability and security should increasingly be considered together. A digitally connected construction system may improve resource efficiency while simultaneously increasing exposure to cyber threats. Conversely, a highly secure system may require additional computing and communication resources that affect its environmental footprint.

This creates a need for integrated evaluation frameworks. Such frameworks should consider at least five dimensions: technological performance, cybersecurity, privacy, environmental sustainability, and economic resilience.

Technological performance includes automation, accuracy, reliability, interoperability, and processing efficiency. Cybersecurity includes authentication, integrity, access control, attack resistance, and system resilience. Privacy concerns the protection of personal, organizational, and commercially sensitive information. Environmental sustainability includes material efficiency, waste reduction, energy consumption, and lifecycle impacts. Economic resilience includes cost control, supply continuity, and adaptability to market disruptions.

The VANET literature demonstrates how authentication, pseudonym management, Sybil resistance, zero trust, and decentralized trust can be combined to create more secure digital ecosystems [5–23]. The construction literature demonstrates how digital inspection, automated fabrication, sustainable materials, and supply-chain management can improve infrastructure efficiency and sustainability [1–4]. Combining these perspectives provides a foundation for developing infrastructure systems that are simultaneously intelligent, secure, and sustainable.

3.11 Comparative Synthesis

The two technological domains reviewed in this study differ substantially in their immediate objectives but share several underlying principles.

In connected vehicles, the primary concerns are secure communication, privacy, authentication, accountability, and resistance to malicious behavior [5–23]. In construction, the primary concerns include quality management, automated fabrication, material sustainability, and supply-chain resilience [1–4].

Nevertheless, both domains rely on trustworthy digital information. A VANET requires reliable identity and communication information to make safe decisions, while an intelligent construction system requires reliable inspection, material, design, and supply-chain information. In both cases, data manipulation can produce physical and economic consequences.

Both domains also require resilience. In VANETs, resilience involves maintaining secure communication despite malicious participants or network disruptions. In construction, resilience involves maintaining project continuity despite material shortages, price volatility, technical failures, or information disruptions [4].

Another common feature is the increasing importance of distributed systems. Connected vehicles communicate across vehicles, RSUs, cloud platforms, and service providers [18,19]. Construction projects similarly involve distributed participants including contractors, suppliers, consultants, inspectors, designers, and project owners. This distribution creates opportunities for collaboration but also increases the need for authentication, authorization, data governance, and interoperability.

3.12 Research Gaps in Intelligent and Sustainable Construction

Several research gaps emerge from the reviewed construction studies.

First, further research is required to integrate digital inspection with predictive quality management. Existing digital inspection approaches provide valuable data, but greater use of historical inspection information and predictive analytics could help identify potential defects before they become costly.

Second, the sustainability performance of 3D-printed concrete requires broader lifecycle evaluation. Future studies should consider material production, energy consumption, transportation, printing, curing, maintenance, and end-of-life impacts rather than evaluating printing efficiency in isolation [2].

Third, sustainable concrete research should increasingly integrate digital optimization with lifecycle environmental assessment. The combination of recycled aggregates and supplementary cementitious materials should be assessed simultaneously according to strength, durability, cost, embodied environmental impact, and service life [3].

Fourth, construction supply chains require more adaptive digital risk-management mechanisms. Predictive models should incorporate market, supplier, transportation, and material-availability information to support proactive decision-making [4].

Fifth, cybersecurity remains underdeveloped in many construction digitalization initiatives. As project data become increasingly interconnected, security mechanisms such as strong authentication, role-based authorization, zero-trust principles, secure data exchange, and tamper-resistant records require greater attention.

Finally, there is a need for common evaluation frameworks that simultaneously measure sustainability and digital security. Current research often evaluates technological performance and environmental performance separately. Future infrastructure systems require integrated metrics that reveal whether a digital solution improves efficiency without creating unacceptable cybersecurity, privacy, energy, or lifecycle costs.

4. Discussion

The review demonstrates that digital transformation is reshaping infrastructure through the integration of connected systems, intelligent technologies, automated processes, data-driven decision-making, and sustainable practices. Although connected transportation and intelligent construction have developed as relatively distinct research areas, both increasingly depend on digital information, interconnected devices, distributed platforms, and automated decision-making. This creates a common need for secure, reliable, interoperable, and resilient digital infrastructure.

One of the main findings is that digital transformation creates both opportunities and risks. Digital technologies can improve operational efficiency, quality control, resource utilization, communication, and decision-making. However, greater connectivity also increases dependence on digital systems and creates additional exposure to cyberattacks, unauthorized access, data manipulation, privacy violations, and system failures. Therefore, digitalization should not be evaluated only according to its technological capabilities. Its reliability, security, environmental performance, and long-term operational resilience should also be considered.

Privacy represents an important challenge in connected infrastructure. Modern digital systems continuously generate information about users, vehicles, locations, transactions, construction activities, suppliers, and organizational processes. Protecting such information while maintaining sufficient accountability is a complex requirement. Excessive anonymity may make it difficult to identify malicious activities, whereas excessive traceability may create privacy risks. Future infrastructure systems should therefore adopt balanced approaches that protect legitimate users while providing appropriate mechanisms for accountability.

Another important issue is interoperability. Digital infrastructure involves multiple devices, software platforms, organizations, communication technologies, and data formats. If these systems cannot exchange information effectively, the benefits of digitalization become limited. Connected vehicles may need to interact with roadside infrastructure, cloud services, traffic-management systems, and external mobility platforms. Similarly, construction environments may involve designers, contractors, suppliers, inspectors, equipment, project-management systems, and digital monitoring platforms. Common data structures, secure interfaces, and interoperable architectures are therefore essential.

Scalability is also a significant research challenge. The number of connected devices and the volume of generated data are expected to increase substantially. Digital infrastructure must be capable of processing large quantities of information without creating excessive communication, computational, storage, or energy requirements. Security mechanisms must also remain effective when deployed across large and heterogeneous environments.

The relationship between digitalization and sustainability requires greater attention. Digital technologies can reduce material waste, improve process efficiency, optimize resource utilization, and support better planning. However, digital systems themselves require hardware, electricity, communication networks, data centers, and computational resources. Therefore, the environmental benefits of digitalization should be evaluated against its complete lifecycle requirements. Future studies should consider both the sustainability benefits enabled by digital technologies and the environmental costs associated with operating those technologies.

A further research gap concerns the limited integration of cybersecurity and sustainability assessment. Security and sustainability are often treated as separate objectives. A more comprehensive approach would evaluate whether a digital solution can provide adequate protection while maintaining reasonable energy consumption, environmental performance, economic feasibility, and operational efficiency. This integrated perspective is particularly important for infrastructure systems expected to operate continuously over long periods.

Real-world implementation is another important challenge. Many emerging digital technologies are demonstrated through conceptual frameworks, simulations, laboratory experiments, or controlled environments. However, real infrastructure systems operate under uncertain and changing conditions. They involve human users, equipment failures, communication disruptions, environmental influences, organizational constraints, and unexpected security events. Greater emphasis should therefore be placed on field demonstrations, long-term monitoring, and large-scale deployment.

The human and organizational dimensions of digital transformation also require greater consideration. Technology adoption depends on user skills, training, organizational culture, management support, financial resources, and willingness to modify established processes. A technically advanced system may provide limited benefits if users cannot operate it effectively or if organizations are unwilling to integrate it into existing workflows. Digital transformation should therefore be regarded as an organizational change process rather than simply a technology implementation exercise.

Overall, the research gap lies in the absence of sufficiently integrated approaches that combine digital intelligence, cybersecurity, privacy, sustainability, resilience, interoperability, and economic feasibility. Future research should move beyond isolated technological solutions and develop infrastructure architectures capable of addressing these requirements simultaneously.

5. Conclusions

Digital transformation is becoming a fundamental component of modern infrastructure development. Connected transportation and intelligent construction represent two important areas in which digital technologies are changing the way infrastructure is designed, operated, monitored, and managed. The integration of digital systems provides opportunities to improve efficiency, quality, safety, sustainability, and resilience, but it also creates new technological and organizational challenges.

The review indicates that future infrastructure should be designed as an integrated physical-digital ecosystem. Such systems should combine physical assets with sensing technologies, secure communication, intelligent analytics, automated decision-making, and effective management processes. Security and privacy should be incorporated from the initial design stage rather than treated as additional features after system deployment.

Sustainability should similarly become an integral part of digital infrastructure planning. Future technologies should be evaluated according to material consumption, energy requirements, environmental impacts, lifecycle performance, and economic feasibility. Digital technologies should contribute to sustainability without creating disproportionate environmental burdens through excessive computing, communication, or hardware requirements.

Future research should focus on the integration of artificial intelligence, edge computing, digital twins, advanced sensing, secure communication, and predictive analytics. Artificial intelligence can support real-time anomaly detection, predictive maintenance, construction-quality assessment, resource optimization, and supply-chain forecasting. Edge computing can enable faster processing closer to physical infrastructure, reducing communication delays and unnecessary data transfer. Digital twins can provide continuous digital representations of physical assets and support lifecycle monitoring and decision-making.

Privacy-preserving data analytics is another promising direction. Future infrastructure will generate increasingly large quantities of sensitive information, making it important to develop methods that allow data to be analyzed without unnecessary disclosure of personal or organizational information. Secure distributed analytics can support collaboration between multiple organizations while maintaining appropriate control over sensitive information.

Energy-efficient security should also become a major research priority. Advanced authentication, continuous monitoring, distributed computing, and data-processing mechanisms can require substantial computational resources. Future security technologies should therefore achieve an appropriate balance between protection, computational efficiency, energy consumption, and system performance.

Another important direction is the development of standardized evaluation frameworks. Future studies should assess digital infrastructure using consistent technical, security, environmental, economic, and operational indicators. Such frameworks would allow researchers and infrastructure managers to compare alternative technologies more objectively and identify solutions that provide the greatest overall value.

Long-term field validation should also receive greater attention. Technologies that perform well under controlled conditions may encounter different challenges when deployed across complex infrastructure environments. Real-world testing can reveal issues related to scalability, interoperability, user acceptance, maintenance, cybersecurity, environmental conditions, and operational reliability.

The future development of infrastructure will therefore depend on the convergence of secure connectivity, intelligent decision-making, sustainable technologies, and resilient management.

References

[1] Parikh, P. B. (2026). Implementing digital inspection protocols for enhanced quality control management in high-rise construction. *Power System Protection and Control*, 54(3), 147–163. https://doi.org/10.46121/pspc.54.3.12

[2] Parikh, P. B. (2026). Evaluating the feasibility and efficiency of 3D-printed concrete technology in sustainable modular construction. *Power System Protection and Control*, 54(1), 887–900. https://doi.org/10.46121/pspc.54.1.61

[3] Parikh, P. B. (2025). Optimizing the structural and durability performance of concrete using recycled aggregates and supplementary cementitious materials. *Power System Protection and Control*, 53(4), 564–576. https://doi.org/10.46121/pspc.53.4.39

[4] Parikh, P. B. (2025). Frameworks for mitigating supply chain disruptions and material price volatility in sustainable building construction. *Power System Protection and Control*, 53(2), 410–426. https://doi.org/10.46121/pspc.53.2.34

[5] Akil, M., Martucci, L. A., & Hoepman, J.-H. (2023). Non-interactive privacy-preserving Sybil-free authentication scheme in VANETs. In *Inaugural International Symposium on Vehicle Security and Privacy (VehicleSec 2023)*. Internet Society. https://doi.org/10.14722/vehiclesec.2023.23007

[6] Akil, M., Martucci, L. A., & Hoepman, J.-H. (2024). A secure and privacy-preserving authentication scheme with a zero-trust approach to vehicle renting in VANETs. In *Proceedings of the 21st International Conference on Security and Cryptography (SECRYPT 2024)*, 114–127. SCITEPRESS. https://doi.org/10.5220/0012759600003767

[7] Akil, M., Naskar, S., Martucci, L. A., & Hoepman, J.-H. (2024). A privacy-preserving approach to vehicle renting and driver accountability in VANETs. In *Privacy and Identity Management. Sharing in a Digital World: 18th IFIP WG 9.2, 9.6/11.7, 11.6 International Summer School, Privacy and Identity 2023, Revised Selected Papers*, 192–210. Springer. https://doi.org/10.1007/978-3-031-57978-3_13

[8] Akil, M., Mancini, L. V., & Venturi, D. (2019). Multi-covert channel attack in the cloud. In *Proceedings of the 6th International Conference on Software Defined Systems (SDS 2019)*, 160–165. IEEE. https://doi.org/10.1109/SDS.2019.8768563

[9] Zeng, M., & others. (2019). Mix-context-based pseudonym changing privacy preserving authentication in VANETs. *Mobile Information Systems*, 2019, 3109238. https://doi.org/10.1155/2019/3109238

[10] Wu, L., Fan, J., Xie, Y., Wang, J., & Liu, Q. (2017). Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks. International Journal of Distributed Sensor Networks, 13(3), 1550147717700899. https://doi.org/10.1177/1550147717700899

[11] Rajput, U., Abbas, F., Eun, H., Hussain, R., & Oh, H. (2015). A two level privacy preserving pseudonymous authentication protocol for VANET. In 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 643–650. IEEE. https://doi.org/10.1109/WiMOB.2015.7348023

[12] Chowdhury, M., Gawande, A., & Wang, L. (2017). Anonymous authentication and pseudonym-renewal for VANET in NDN. In Proceedings of the 6th ACM Conference on Information-Centric Networking (ICN 2017). ACM. https://doi.org/10.1145/3125719.3132111

[13] Benarous, L., Kadri, B., Bitam, S., & Mellouk, A. (2020). Privacy-preserving authentication scheme for on-road on-demand refilling of pseudonym in VANET. *International Journal of Communication Systems*, 33(10). https://doi.org/10.1002/dac.4087

[14] Mundhe, P., Verma, S., & Venkatesan, S. (2021). A comprehensive survey on authentication and privacy-preserving schemes in VANETs. *Computer Science Review*, 41, 100411. https://doi.org/10.1016/j.cosrev.2021.100411

[15] Alazzawi, A. K., et al. (2020). Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs). *Vehicular Communications*, 25, 100247. https://doi.org/10.1016/j.vehcom.2020.100247

[16] Kerson, J., & Anita, M. (2022). Secure authentication schemes for vehicular adhoc networks: A survey. *Wireless Personal Communications*, 123, 261. https://doi.org/10.1007/s11277-021-09118-3

[17] Ahmed, W., & Wu, D. (2022). Privacy-preserving blockchain-based authentication and trust management in VANETs. *IET Networks*. https://doi.org/10.1049/ntw2.12036

[18] Stephen, S. M., & Jaekel, A. (2022). Roadside unit-based pseudonym authentication in vehicular ad hoc network. *Security and Privacy*, 5(5), e238. https://doi.org/10.1002/spy2.238

[19] Dwivedi, S. K., Amin, R., Das, A. K., Leung, M. T., Choo, K.-K. R., & Vollala, S. (2022). Blockchain-based vehicular ad-hoc networks: A comprehensive survey. *Ad Hoc Networks*, 137, 102980. https://doi.org/10.1016/j.adhoc.2022.102980

[20] Li, X., et al. (2022). A pseudonym-based certificateless privacy-preserving authentication scheme for VANETs. *Vehicular Communications*, 38, 100535. https://doi.org/10.1016/j.vehcom.2022.100535

[21] Alshammari, M., et al. (2022). PAS: Privacy-preserving authentication scheme based on SDN for VANETs. *Applied Sciences*, 12(9), 4791. https://doi.org/10.3390/app12094791

[22] Ahmed, W., et al. (2021). An efficient privacy-preserving authentication model based on blockchain for VANETs. *Journal of Systems Architecture*, 117, 102158. https://doi.org/10.1016/j.sysarc.2021.102158

[23] Alzahrani, B., et al. (2023). Privacy-preserving authentication scheme for VANETs using blockchain technology. *Procedia Computer Science*, 220, 40–47. https://doi.org/10.1016/j.procs.2023.03.008